全国高等职业教育计算机类规划教材·工作过程系统化教程系列

Windows Server 2003 网络管理项目实训教程

褚建立　主编

路俊维　文玉锋　刘彦舫　副主编

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书作者总结了多年的计算机网络工程实践及高职教学的经验，根据网络工程实际工作过程所需要的知识和技能抽象出 15 个教学项目。按照学习领域的课程教学改革思路进行教材的编写，以工作过程为导向，按照项目的实际实施过程来完成，是为高职院校学生量身定做的教材。

通过这 15 个教学项目的实施，本书内容涵盖了 Windows Server 2003 的安装、配置、管理、各种网络功能和安全功能的实现，以学生能够完成中小企业局域网内常见服务器管理任务为目标。

本书突出对职业能力、实践技能的培养，采用项目驱动模式，设计了丰富的典型工作情境下的工作案例，步骤清晰，图文并茂，应用性强。

本书既可以作为高职院校计算机应用专业和网络技术专业理论与实践一体化教材使用，也可以作为 Windows Server 2003 系统管理和网络管理的自学指导书。

图书在版编目(CIP)数据

Windows Server 2003 网络管理项目实训教程 / 褚建立主编.—北京：电子工业出版社，2009.5
全国高等职业教育计算机类规划教材·工作过程系统化教程系列
ISBN 978-7-121-08679-3
I. W… Ⅱ. 褚… Ⅲ. 服务器—操作系统（软件），Windows Server 2003—高等学校：技术学校—教材
Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字（2009）第 060256 号

策划编辑：左　雅
责任编辑：左　雅
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：18.5　字数：474 千字
印　　次：2009 年 5 月第 1 次印刷
印　　数：4 000 册　定价：28.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

Windows 操作系统不仅仅是当今的主流桌面操作系统，由于其操作直观、简便，Windows 的服务器也成为当前中小企业首选的服务器操作系统。Windows Server 2003 是在 Windows Server 2000 的基础上发展而来的，系统更加稳定，功能更加强大。

本书特色如下：

在组织方式上，按照学习领域的课程改革思路进行教材的组织编写，以工作过程为导向，按照项目的实际实施过程来完成。

在目标上，以适应高职高专教学改革的需要为目标，充分体现高职特色，有所创新和突破，全书的 15 个工作任务均来自企业工程实际。

在内容选取上，坚持集先进性、科学性和实用性为一体，尽可能选取最新、最实用的技术，与当前企业实际需要的网络技术接轨。

在教材内容深浅程度上，把握理论够用、侧重实践、由浅入深的原则，以使学生分层分步骤掌握所学的知识。

在教材结构上，本书共分为 15 个教学项目。在每个教学项目中，先提出工作任务，然后提供完成工作任务所应掌握的相关知识和操作技能，在学习知识的前提下进行方案分析，从而实施完成任务并进行测试。

通过 Windows Server 2003 的安装与配置，工作组模式下的用户、组、文件管理，磁盘管理，网络打印的配置与管理，域模式，域用户及组的管理、架设单位内部 DNS 并提供域名解析服务，利用 DHCP 自动分配 IP 地址，利用 IIS 架设单位内部 Web 服务器，架设单位内部 FTP 服务器，电子邮件服务，安装和配置终端服务，使用 WSUS 升级操作系统补丁，VPN 服务器的配置与管理，Windows Server 2003 性能监视和优化等教学项目，来完成对 Windows Server 2003 的学习。

本书建议教学课时数为 72 课时，其中讲授 36 课时、实践 36 课时。

本书由邢台职业技术学院褚建立组织编写并统稿，路俊维、文玉锋、刘彦舫任副主编。其中项目 6、7、8 由褚建立组织编写，项目 3、4、14 由路俊维编写，项目 1、2、5 由西北师范大学文玉锋编写，项目 15 由刘彦舫编写，项目 9 由邵慧莹编写，项目 12 由辛景波编写，项目 13 由高欢编写，项目 11 由曹新鸿编写，项目 10 由曾凡晋编写。

由于时间仓促，加上作者水平有限，书中难免有不妥和错误之处，恳请广大读者指正。E-mail：xpcchujl@126.com。

编　　者

目　录

项目 1　Windows Server 2003 安装与配置

1.1　项目内容

1．项目目的

通过安装 Windows Server 2003 网络操作系统，了解常见的网络操作系统，掌握在 Windows Server 2003 中分区的方法和文件系统的选择，掌握 Windows Server 2003 的安装方法。

2．项目任务

某高校，组建了学校的校园网，开发了各学院的主页，需要架设一台具有 Web、FTP、DNS、DHCP 等功能的服务器来为校园网用户提供服务，现需要选择一种既安全又易于管理的的网络操作系统。

3．任务目标

① 学会在一台 PC 计算机上安装 Windows Server 2003；
② 学会将计算机系统从 Windows Server 2000 升级到 Windows Server 2003；
③ 学会制作 Windows Server 2003 自动安装光盘。

1.2　相关知识

1.2.1　网络操作系统概述

1．网络操作系统的定义和功能

网络操作系统（Network Operation System，NOS）是指能使网络上多台计算机方便而有效地共享网络资源，为用户提供所需的各种服务的操作系统软件。

为实现有效的资源共享，首先要提供网络通信功能或协议的支持，另外还要提供资源共享的途径，以及解决多个用户对资源需求冲突的能力。所以网络操作系统除了具备单机操作系统所需的功能（如内存管理、CPU 管理、输入/输出管理、文件管理等）以外，还应具备如下一些网络控制、管理和服务功能。

- 提供高效可靠的网络通信能力，如对网络协议、网络硬件的支持。例如，在 Windows 2000/2003 操作系统中，就有对 TCP/IP、NetBEUI、DLC 等多种协议的支持，同时还提供了多种网络硬件的驱动程序。
- 提供多项网络服务功能，如远程作业录入及处理的服务功能、文件传输服务功能、电子邮件服务功能、远程打印服务功能等。大家熟知的 Telnet、FTP、E-mail 等就是该类服务功能的典型例子。
- 提供网络资源管理、系统管理功能，如文件系统管理、网络服务进程的建立和管理、网络活动的监控和网络测试工具等。Windows 2000/2003 中的事件查看器就提供对一

些网络安全方面的问题进行监视的功能。

- 提供对网络用户的管理。几乎所有的操作系统都提供了用户管理功能，用户管理功能所提供的用户访问控制机制有效地管理和控制了用户对网络资源的访问。用户必须提供合法的用户账号并在授权范围内访问网络资源就是用户管理的具体体现。

2．网络操作系统的组成

网络操作系统通常有两个基本的组成部分，即运行在服务器上的操作系统和运行在每个PC 或桌面工作站上的客户端操作系统。服务器操作系统的主要功能是控制服务器的操作，管理存储在服务器上的文件，提供对用户的集中管理，支持多用户和多任务的工作环境，以解决多个用户对资源需求时的冲突。客户端操作系统的主要功能是提供给客户访问网络及网络资源的能力，而这些网络资源通常由网络服务器提供。

1.2.2 常见的网络操作系统

网络操作系统是在网络设计与实施过程中要考虑的关键因素之一。目前，可供选择的网络操作系统多种多样，常见的有 Windows、UNIX、Linux、NetWare 等。

1．Windows操作系统

Windows 的网络操作系统是一个产品系列。微软公司在 1993 年推出了第一代网络操作系统产品 Windows NT 3.1。随着 Windows NT 3.1 的问世，微软正式加入网络操作系统的市场角逐。时至今日，微软公司先后对 Windows 网络操作系统进行了多次改进，陆续推出了 Windows NT 3.5、Windows NT 4.0、Windows Server 2000 家族，以及现在的 Windows Server 2003/2008。Windows 网络操作系统具有较高的可靠性，采用最新的概念和最新的技术，具有友好的界面，具有丰富的配套应用。

正是由于具备上述优越的性能，使得微软的 Windows 网络操作系统系列产品后来居上，在当今的网络操作系统市场占有举足轻重的地位。

2．UNIX操作系统

UNIX 最早是指由美国贝尔实验室发明的一种多用户、多任务的通用操作系统。经过长期的发展和完善，目前已成长为一种主流的操作系统技术和基于这种技术的产品大家族，其中最为著名的有 SCO XENIX、SNOS、Berkeley BSD、AT&T UNIX 系统。由于 UNIX 具有技术成熟、可靠性高、网络和数据库功能强、伸缩性突出和开放性好等特色，可满足各行各业的实际需要，特别能满足企业重要业务的需要，已经成为主要的工作站平台和重要的企业操作平台。

3．Linux操作系统

Linux 是一个免费的、开放源代码的操作系统。Linux 脱胎于 UNIX，所以其很多性能和特点与 UNIX 极其相似。Linux 最早出现在 1992 年，由芬兰赫尔辛基大学学生 Linus B.Torvolds 首创，后来在世界各地由成千上万的 Internet 上的自由软件开发者通过互联网协同开发，并不断完善。经过十多年的发展，它已完全进入了成熟阶段，越来越多的人认识到它的价值，从因特网服务器到用户的桌面，从图形工作站到 PDA 的各种领域都在广泛使用。Linux 下有大量的免费应用软件，如系统工具、开发工具、网络应用、休闲娱乐、游戏等。更重要的是，它是目前安装在个人电脑上的最可靠、最稳定的操作系统。

Linux 作为一个置于共用许可证（General Public License，GPL）保护下的自由软件，任何人都可以免费下载。目前 Linux 的发行版本种类很多，最主要的几个发行版本为：Red Hat Linux、Slackware、Debian Linux、S.u.S.e Linux 等。最近在国内也有公司开发了自己的发行版本，如联想公司的幸福 Linux 和冲浪平台的 Xteam Linux。

4．NetWare操作系统

Novell 公司的 NetWare 网络操作系统是目前世界上应用最广泛的微型计算机局域网络操作系统之一。

NetWare 的推出时间比较早，经过多年的发展，已具有非常稳定的运行性能。在一个 NetWare 网络中允许有多个服务器，并可采用一般的 PC 担当服务器。NetWare 网络操作系统具有强大的文件及打印服务能力、兼容性及系统容错能力、比较完备的安全措施等。

1.2.3 Windows Server 2003 的版本

微软公司在 2003 年 4 月发布了 Windows Server 2003 操作系统，沿用了 Windows Server 2000 家族的版本划分方式，包括 Windows Server 2003 标准版、Windows Server 2003 企业版和 Windows Server 2003 数据中心版。除此以外，为了降低成本，Windows Server 2003 还专门提供了网络版本，作为部门或小型企业服务器使用。

1．Windows Server 2003 标准版

Windows Server 2003 标准版是一个可靠的网络操作系统，可迅速方便地提供企业解决方案。这种灵活的服务器是小型企业和部门应用的理想选择。Windows Server 2003 标准版具有以下特点：

- 支持文件和打印机共享；
- 提供安全的 Internet 连接；
- 允许集中化的桌面应用程序部署。

2．Windows Server 2003 企业版

Windows Server 2003 企业版是为满足各种规模的企业的一般用途而设计的。它是各种应用程序、Web 服务和基础结构的理想平台，能够提供高度可靠性、高性能和出色的商业价值。Windows Server 2003 企业版具有以下特点：

- 是一种全功能的服务器操作系统，支持多达 8 个处理器；
- 提供企业级功能，如 8 节点群集、支持高达 32GB 内存等；
- 可用于基于 Intel Itanium 系列的计算机；
- 将可用于能够支持 8 个处理器和 64GB RAM 的 64 位计算平台。

3．Windows Server 2003 数据中心版

Windows Server 2003 数据中心版是为运行企业和任务所倚重的应用程序而设计的，这些应用程序需要最高的可伸缩性和可用性。Windows Server 2003 数据中心版具有以下特点：

- 是微软迄今为止开发的功能最强大的服务器操作系统；
- 支持高达 32 路的 SMP 和 64GB 的 RAM；
- 提供 8 节点群集和负载平衡服务是它的标准功能；
- 将可用于能够支持 32 个处理器和 128GB RAM 的 64 位计算平台。

4．Windows Server 2003 网络版

Windows 操作系统系列中的新产品，Windows Server 2003 网络版用于 Web 服务和托管。Windows Server 2003 网络版具有以下特点：

- 用于生成和承载网络应用程序、网络页面以及 XML Web 服务；
- 其主要目的是作为 IIS 6.0 网络服务器使用；
- 提供一个快速开发和部署 XML 网络服务和应用程序的平台，这些服务和应用程序使用 ASP.NET 技术，该技术是.NET 框架的关键部分；
- 便于部署和管理。

表 1.1 为不同版本的主要性能比较。

表 1.1　Windows Server 2003 版本的主要性能比较

性　能	网　络　版	标　准　版	企　业　版	数据中心版
支持 64 位 CPU	否	否	是	是
支持内存量	2GB	4GB	32GB/32 位 64GB/64 位	64GB/32 位 128GB/64 位
SMP CPU 数	2	4	8	32/32 位 64/64 位
活动目录服务	否	是	是	是

1.3　方案设计及准备

1．设计

根据前面的介绍，我们在为学校选择网络操作系统时，首先推荐 Windows Server 2003 操作系统。在安装 Windows Server 2003 操作系统时要求如下：

从光盘安装 Windows Server 2003，设置相应的信息。计算机名为 xpc-xxgcx-jpkc，IP 地址为 192.168.1.100，子网掩码为 255.255.255.0，默认网关为 192.168.1.1，DNS 为 202.99.16.68，系统管理员密码为 qazWSXedc123456，授权模式为每服务器模式，用户数为 200 个，文件系统采用 NTFS，C 盘分区在 5GB 以上，安装完后为独立服务器。

2．设备清单

① PC 计算机 1 台；

② Windows Server 2003 Standard Edition 简体中文标准版安装光盘。

3．Windows Server 2003 简体中文版安装准备

为了安装 Windows Server 2003 服务器，需要准备好 Windows Server 2003 Standard Edition 简体中文标准版安装光盘。用纸张记录安装文件的产品密匙（安装序列号）。规划启动盘的大小。主要内容包括：

（1）准备好 Windows Server 2003 Standard Edition 简体中文标准版安装光盘。

（2）在可能的情况下，在运行安装程序前用磁盘扫描程序扫描所有硬盘，检查硬盘错误并进行修复，否则安装程序运行时如检查到有硬盘错误会很麻烦。

（3）用纸张记录安装文件的产品密匙（安装序列号）。

（4）如果未安装过 Windows Server 2003 系统，而现在正使用 Windows XP/2000 系统，建议用驱动程序备份工具（如：驱动精灵 2004 V1.9 Beta.exe）将 Windows XP/2000 系统下的所有驱动程序备份到硬盘上（如：F:\Drive）。备份的 Windows XP/2000 系统驱动程序可以在 Windows Server 2003 系统下使用。

（5）如果想在安装过程中格式化 C 盘或 D 盘（建议安装过程中格式化用于安装 Windows Server 2003 系统的分区），需要备份 C 盘或 D 盘有用的数据。

（6）导出电子邮件账户和通讯簿：将“C:\Documents and Settings\Administrator（或你的用户名）\”中的“收藏夹”目录复制到其他盘，以备份收藏夹。

（7）系统要求：对基于 X86 的计算机，建议使用一个或多个主频不低于 1.0GHz（支持的最低主频为 133MHz）的处理器，每台计算机最多支持 8 个处理器。建议使用 Intel Pentium4/Celeron/Athlon/Duron 系列或兼容的处理器。建议最少使用 512MB 的 RAM，最大支持 32GB。硬盘可用空间大约为 1.25～2GB，如果通过网络而不是 CD-ROM 运行安装程序，或者从 FAT 或 FAT32 分区执行升级（推荐使用 NTFS 文件系统），那么将需要更大的磁盘空间。

1.4 项目实施

1.4.1 全新安装

步骤 1：用光盘启动系统。因为需要从光驱引导进行安装，所以重新启动系统并设置计算机的 BIOS，把光驱（CD－ROM）设为第一启动盘，保存设置并重新启动。将 Windows Server 2003 安装光盘放入光驱，重新启动计算机。刚启动时，当屏幕出现“Press any Key to boot from CD..”字样时，按任意键从光驱引导，否则不能启动 Windows Server 2003 系统安装。

步骤 2：按任意键，系统从光驱引导。安装程序会将 Windows Server 2003 核心程序、安装时所需要的文件等加载到内存后，开始加载各种驱动程序。如果系统发现有无法识别的 RDID 控制器，可按 F6 手工添加；按 F3 键可以退出安装。

步骤 3：驱动程序加载结束后，屏幕出现安装程序欢迎界面，如图 1.1 所示。在这里提供两种安装方式：第 1 种是现在安装，适合于全新安装，按 Enter 键开始安装；第 2 种是修复安装，适合于系统出现故障后通过“还原控制台”进行修复安装，按 R 键开始安装。选择第 1 种安装方式。

步骤 4：按 Enter 键，出现授权协议画面，如图 1.2 所示。

步骤 5：按 Page Up 或 Page Down 键浏览授权协议的内容，按 F8 键同意 Windows 许可协议。如果之前没有安装其他的操作系统，则弹出“磁盘分区情况”界面，如图 1.3 所示。在该画面中可以对磁盘进行重新分区或者创建新的分区。要创建新的分区，用上下箭头键选择“未划分的空间”后按 C 键，弹出如图 1.4 所示画面，输入分区的大小后按 Enter 键。

如果之前安装有其他的操作系统，则弹出选择安装磁盘分区画面，如图 1.5 所示。如果删除原有的分区将会导致原有分区上数据的丢失。要删除分区，则选择相应的分区后按 D 键，再按 L 键确认，如图 1.6 所示。

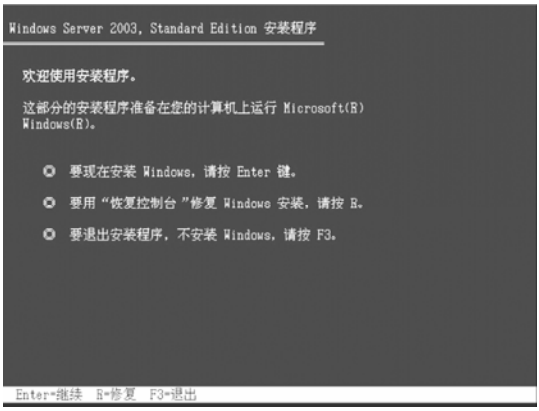

图 1.1　安装程序欢迎界面

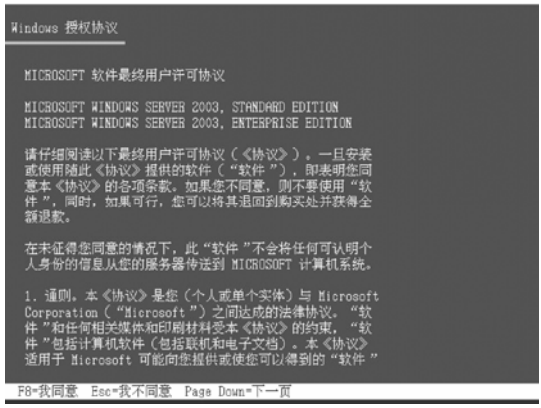

图 1.2　产品授权协议

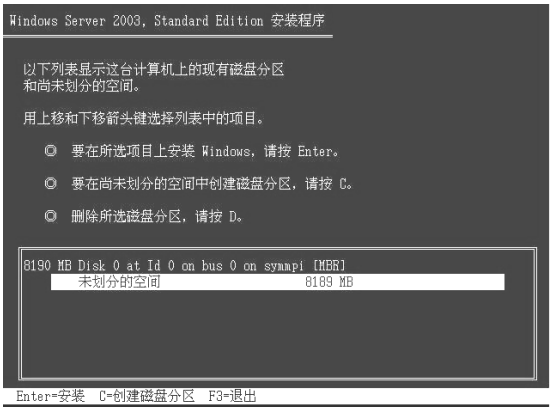

图 1.3　磁盘分区情况

图 1.4　创建分区大小

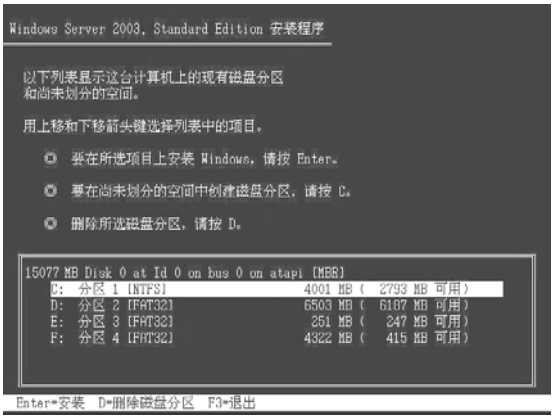

图 1.5　选择安装磁盘分区

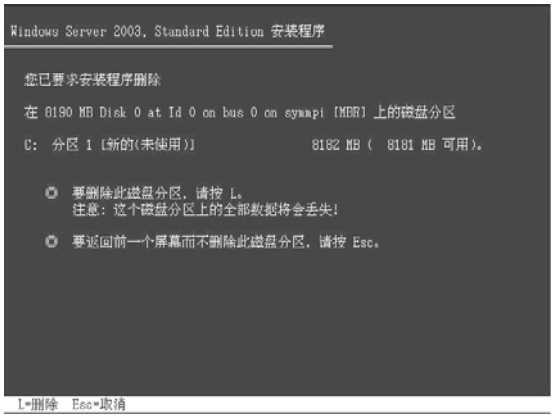

图 1.6　删除分区

步骤 6：用方向键选择安装系统所用的分区，这里准备用 C 盘安装 Windows Server 2003，并准备在下面的过程中格式化 C 盘。选择好分区后按 Enter 键，安装程序将检查 C 盘的空间和 C 盘现有的操作系统。完成后出现如图 1.7 所示画面。

图 1.7 表示安装程序检测到 C 盘已经有操作系统存在，提出警告信息。如果选择安装系统的分区是空的，则不会出现图 1.7 而直接出现如图 1.9 所示画面。

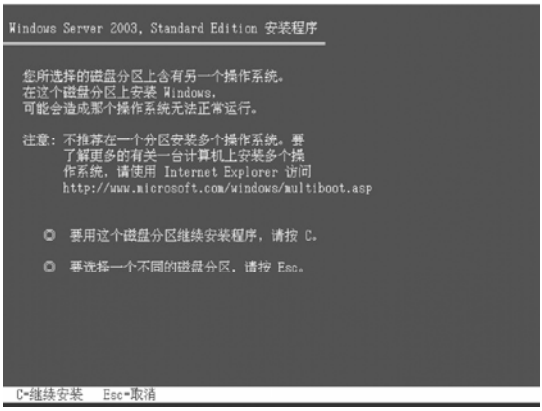

图 1.7　检查 C 盘区

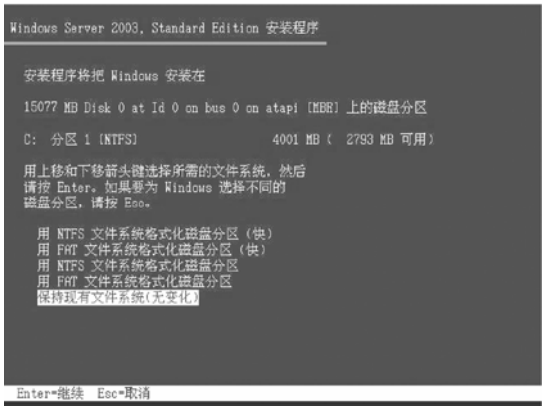

图 1.8　磁盘格式化方式

根据提示，按下键盘上的 C 键后出现如图 1.8 所示界面。在图 1.8 最下方提供了 5 个对所选分区进行操作的选项，其中“保存现有文件系统（无变化）”的选项不含格式化分区操作，其他都会有对分区进行格式化的操作。这里，用“↑”键选择“用 NTFS 文件系统格式化磁盘分区”，如图 1.9 所示。按 Enter 键，出现格式化 C 盘的警告，如图 1.10 所示。

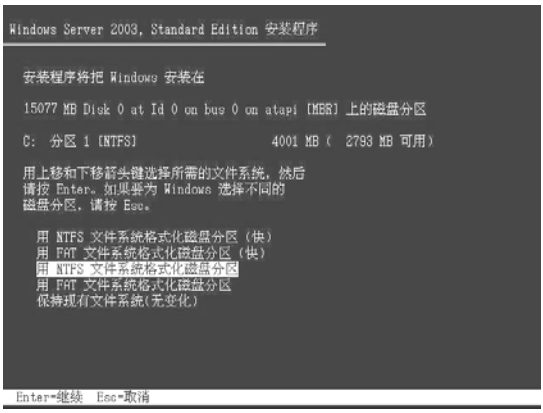

图 1.9　磁盘格式化方式

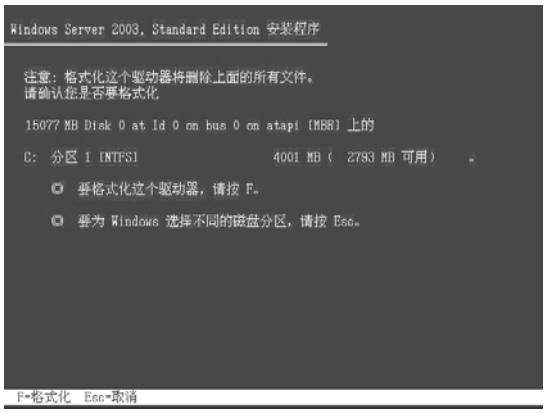

图 1.10　格式化确认

步骤 7：确定要格式化 C 盘后，按 F 键，安装程序将开始格式化 C 盘。只有用光盘启动安装程序，才能在安装过程中提供格式化分区选项；如果用 MS-DOS 启动盘启动进入 DOS 环境，运行 i386\winnt.exe 进行安装时，安装过程没有格式化分区选项。

步骤 8：格式化和分区完成后，创建要复制的文件列表，接着开始复制系统文件。安装程序将从安装光盘中复制必要的安装文件到所选分区的 Windows 安装临时文件夹中。整个复制过程需要花费较长的时间。

步骤 9：文件复制完成后，安装程序开始初始化 Windows 配置。

步骤 10：初始化 Windows 配置完成后，出现系统需要重新启动画面，系统将在 15 秒后重新启动。这时安装程序已经完成，系统将会自动在 15 秒后重新启动，将控制权从安装程序转移给系统。这时建议在系统重新启动时将硬盘设为第一启动盘（不改变也可以）。

步骤 11：重新启动后，首次出现 Windows Server 2003 启动画面。

步骤 12：启动后，安装程序开始检测计算机硬件配置，依次完成收集信息、动态更新、

准备安装、安装 Windows Server 2003 等步骤，后进入 Windows Server 2003 安装画面。

步骤 13：然后，进入“区域和语言选项”界面，并提示安装的剩余时间。用户可以根据需要在安装期间设置“区域和语言选项”，设置数字、货币及日期的显示方式，同时更改系统默认的输入语言和方法，这些也可以在安装完毕后设置。一般“区域和语言选项”设置选用默认值。

步骤 14：直接单击“下一步”按钮，进入“自定义软件”界面，设置个人信息。

步骤 15：输入用户姓名和单位后，单击“下一步”按钮，出现“您的产品密钥”界面，如图 1.11 所示。产品密钥是用户购买 Windows Server 2003 产品时授权许可证上所提供的序列号，用于证明产品的合法性。

步骤 16：输入产品许可证上的产品密钥后，单击“下一步”按钮，出现“授权模式”界面，如图 1.12 所示，选择正确的授权模式。Windows Server 2003 有两种不同的授权模式：每服务器和每设备或每用户。每服务器中，许可证的数量决定了可以同时连接到服务器的用户数量，该模式适用于企业中有许多用户，但只有少量用户会同时访问服务器的场合；在每设备或每用户模式中，许可是为每一用户购买的，有许可的用户可以合法访问企业中的任何一台服务器，不需要考虑用户同时访问多少台服务器，该模式适用于企业中有多台 Windows Server 2003 计算机，并且用户机同时访问服务器的情况。

图 1.11 “您的产品密钥”界面

图 1.12 “授权模式”界面

步骤 17：这里选择“每服务器”模式，输入“每服务器，同时连接数”的值后（这里采用默认值 5），单击“下一步”按钮，进入“计算机名称和管理员密码”界面，如图 1.13 所示。安装程序会自动创建计算机名称，用户可任意更改，输入两次系统管理员密码，记住这个密码。系统管理员在系统中具有最高权限。密码长度少于 6 个字符时会出现如图 1.14 所示的提示信息。密码的设置建议使用英文字母大小写和符号的组合，长度应当在 8 位以上。

步骤 18：输入计算机名称和管理员密码后，单击“下一步”按钮，在弹出的确认窗口中单击“是”按钮，进入“日期和时间设置”界面。

系统的日期和时间来自 CMOS，所以 Windows 系统中的日期和时间设置与 CMOS 一样。

步骤 19：设置好日期、时间和时区后，单击“下一步”按钮，进入“网络设置”界面。一般情况下在安装过程中选择“典型设置”，系统安装完成后再进行手工设置。

图 1.13 “计算机名称和管理员密码”界面

图 1.14 “弱密码提示信息”界面

步骤 20：选择“典型设置”，并单击“下一步”按钮，进入“工作组或计算机域”设置界面，如图 1.15 所示。如果选择第一个选项，则该服务器是工作组 Workgroup 中的一员，即组成对等网；选择第二项则该服务器成为域中的一员，即组成域模式。这里选择第一项即默认选项。

步骤 21：单击“下一步”按钮，计算机自动完成以后的全新安装。

步骤 22：安装完成后自动重新启动，出现启动画面，然后出现欢迎画面。

步骤 23：按 Ctrl+Alt+Delete 组合键后继续启动，出现如图 1.16 所示的登录界面。

图 1.15 “工作组或计算机域”界面

图 1.16 登录界面

步骤 24：输入密码后按 Enter 键，继续启动进入桌面。第一次启动后自动运行“管理您的服务器”向导。

如果不想每次启动都出现这个窗口，可在该窗口左下角的“在登录时不要显示此项”前面打钩然后关闭窗口。关闭该窗口后即见到 Windows Server 2003 的桌面，此时桌面上只有回收站和语言栏。

步骤 25：如果想将主要图标显示到桌面上，可以右击桌面，并在弹出的菜单中选择“属性”。进入“属性”窗口后，选择“桌面”选项卡，单击“自定义桌面”，弹出“桌面项目”窗口，如图 1.17 所示。将“桌面图标”栏中的选项选中，并单击“确定”按钮。

步骤 26：在安装 Windows Server 2003 简体中文版时，默认安装了 Internet Explorer 增强

的安全设置，默认关闭了声音，默认没有开启显示和声音的硬件加速。这样在上网时，大部分网站不能打开，系统无声，播放电影和音乐迟钝。同时默认要按 Ctrl+Alt+Delete 组合键登录，默认开启了关机事件跟踪。

1.4.2 升级安装

从 Windows Server 2000 升级到 Windows Server 2003 非常简单。不需要格式化磁盘原有分区，并能保留原来已安装的应用程序。

从 Windows Server 2000 升级到 Windows Server 2003，安装步骤如下：

步骤 1：打开计算机，并启动到 Windows Server 2000，在光驱中放入 Windows Server 2003 安装光盘，并运行光盘根目录下的安装文件 setup.exe。屏幕出现升级画面，如图 1.18 所示。

图 1.17 设置桌面项目

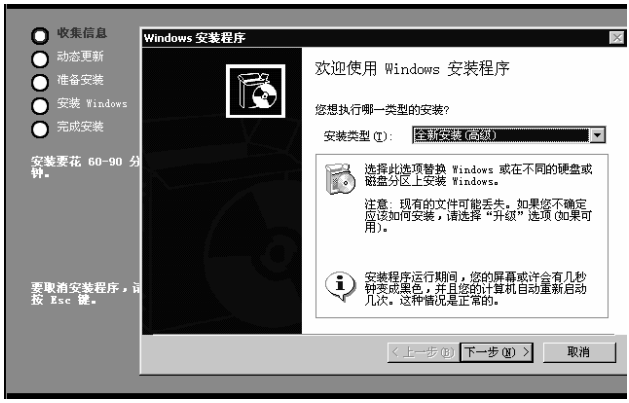

图 1.18 升级安装类型

步骤 2：选择安装类型为“升级”，单击“下一步”按钮，安装程序检测计算机硬件及系统的兼容性，并出现“报告系统兼容性”界面。

步骤 3：单击“下一步”按钮，系统自动安装，不需要用户干预，直至安装完毕。

1.4.3 Windows Server 2003 的自动安装

方法一

步骤 1：解压 support\tools 文件夹内的 deploy.cab 后得到可执行文件 setupmgr.exe。

步骤 2：运行 setupmgr.exe，启动安装管理器，弹出“安装管理器向导”对话框。

步骤 3：单击“下一步”按钮，弹出“新的或现有的应答文件”对话框，选择“创建新文件”，如图 1.19 所示。

步骤 4：单击“下一步”按钮，弹出“安装的类型”对话框，选择“无人参与安装”，如图 1.20 所示。

步骤 5：单击“下一步”按钮，弹出“Windows 产品”对话框，选择“Windows Server 2003 Standard Edition”，如图 1.21 所示。

步骤 6：单击“下一步”按钮，弹出“用户交互”对话框，选择“全部自动”，如图 1.22 所示。

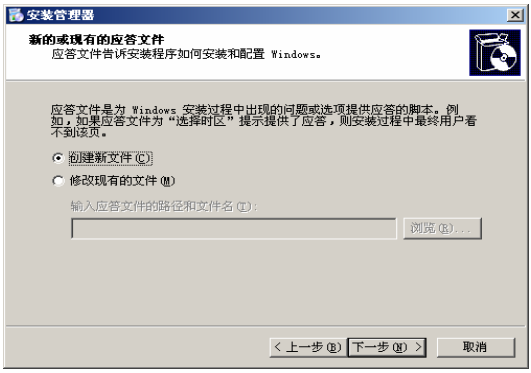

图 1.19 “新的或现有的应答文件”对话框

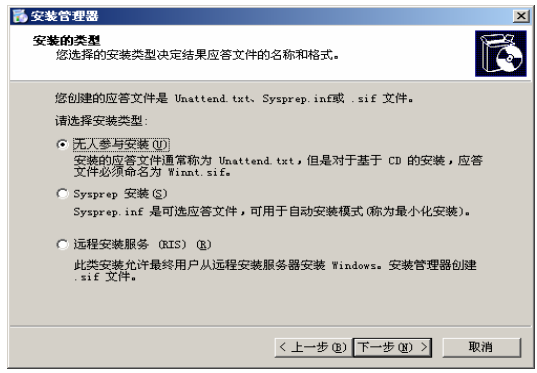

图 1.20 “安装的类型”对话框

图 1.21 “选择 Windows 产品”对话框

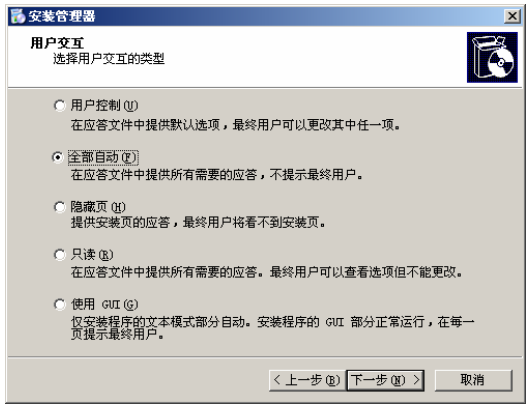

图 1.22 “用户交互”对话框

步骤 7：单击“下一步”按钮，弹出“分布共享”对话框，选择“创建新的分布共享”，如图 1.23 所示。

步骤 8：单击“下一步”按钮，弹出“设置文件的位置”对话框，选择“从 CD”，如图 1.24 所示。

步骤 9：单击“下一步”按钮，弹出“分布共享的位置”对话框，默认设置，如图 1.25 所示。

步骤 10：单击“下一步”按钮，弹出“接受许可协议”对话框，选中接受。

步骤 11：单击“下一步”按钮，弹出“名称和单位”对话框，在“名称”文本框中输入个人名称，在“单位”文本框中输入单位名称，如图 1.26 所示。

步骤 12：单击“下一步”按钮，弹出“显示设置”对话框，接受默认设置。单击“下一步”按钮，弹出“时区”对话框，接受默认设置。

步骤 13：单击“下一步”按钮，弹出“产品密钥”对话框，在“产品密钥”文本框中输入 Windows Server 2003 Standard Edition 购买时的产品密钥。

步骤 14：单击“下一步”按钮，弹出“授权模式”对话框，选择“每服务器模式”，更改同时连接的数目。

步骤 15：单击“下一步”按钮，弹出“计算机名称”窗口，在“计算机名称”栏中输入计算机名称，单击“添加”按钮，加入要安装的计算机中，如图 1.27 所示。

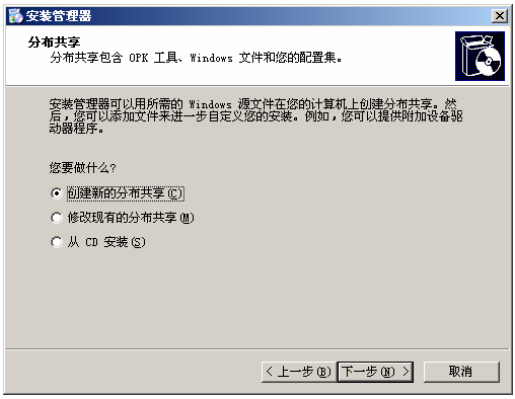

图 1.23 “分布共享”对话框

图 1.24 “设置文件的位置”对话框

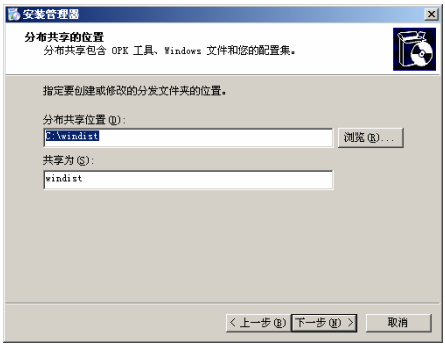

图 1.25 “分布共享的位置”对话框

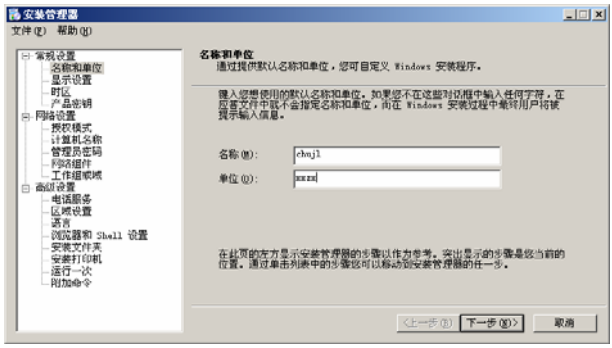

图 1.26 “名称和单位”对话框

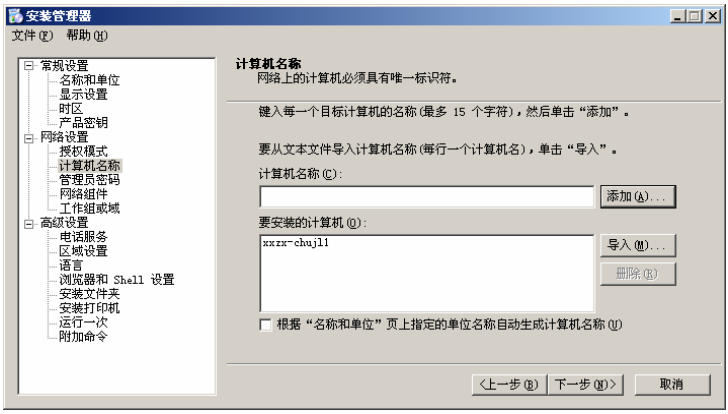

图 1.27 “计算机名称”窗口

步骤 16：依次设置“管理员密码”、“网络组件”、“工作组或域”等所有在安装时所需配置的内容，与 Windows Server 2003 Standard Edition 的全新安装方法一样。

步骤 17：设置完成后，要求输入应答文件保存路径及名称，如图 1.28 所示。单击“确定”按钮继续。

步骤 18：这时，安装程序会把所需的文件复制到指定的分布共享点。复制完成后，会提示已创建的文件。至此，创建应答过程结束。

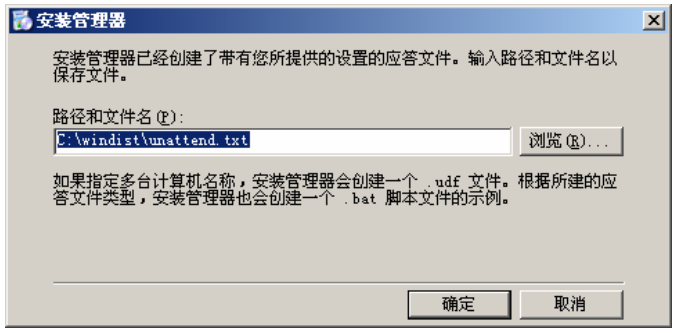

图 1.28　输入保存文件的路径和文件名

安装管理器除了创建应答文件 unattend.txt 外。还会创建一个批处理文件 unattend.bat。用户可以直接运行这个批处理文件来自动安装 Windows 操作系统。

unattend.bat 文件利用 Winnt32.exe 程序安装 Windows 操作系统。只要在命令行提示符状态下输入 unattend 命令，安装程序会自动完成 Windows Server 2003 系统的安装，无须用户干预。

方法二

也可以对安装光盘的 i386 目录下的 unattend.txt 文件进行适当的修改，以“;”开头的为注释行，文件内容如下，其中加下画线的是修改过的内容。

```
; Microsoft Windows
; (c) 1994 - 2001 Microsoft Corporation. All rights reserved.
;
; 无人参与安装应答文件示例
;
; 此文件包含如何自动安装或升级 Windows 的信息，
; 这样安装程序的运行就不需要用户的输入。您可以
; 在 CD:\support\tools\deploy.cab 中的 ref.chm
; 文件中获得更多信息
;
[Unattended]
Unattendmode = FullUnattended
OemPreinstall = NO
TargetPath = *
Filesystem = LeaveAlone

[GuiUnattended]
; 设置时区为中国
; 设置管理员密码为 xpc123456
; 设置 AutoLogon 为 ON 并登录
TimeZone = "210"
AdminPassword = xpc123456
AutoLogon = Yes
AutoLogonCount = 1

[LicenseFilePrintData]
; 授权模式为每服务器模式，用户数为 100 个
AutoMode = "PerServer"
```

```
AutoUsers = "100"

[GuiRunOnce]
; 列出当第一次登录计算机时您想启动的程序

[Display]
BitsPerPel = 32
XResolution = 1024
YResolution = 768
VRefresh = 70

[Networking]

[Identification]
JoinWorkgroup = Infor-depart

[UserData]
FullName = "xpcchujl"
OrgName = "xxgcx"
ComputerName =xxgcx2003-server1

ProductKey = " JDMDG-J6PDP-"T4C4K—MBYQW—98GBB"
```

1.5 扩展知识及任务训练

1.5.1 训练 1：桌面、管理硬件与网络连接

1．整理及设置桌面

刚刚安装好的 Windows Server 2003 的桌面上在右下角只有一个回收站，要在桌面上显示“我的电脑”等图标，操作步骤如下：

① 在桌面空白处单击鼠标右键，选择“属性”，弹出“显示属性”对话框；

② 选择“桌面”选项卡，单击“自定义桌面”按钮，打开“桌面项目”对话框；

③ 在“常规”选项卡中，选中要在桌面显示的图标，例如，“我的电脑”、“网上邻居”、“我的文档”等。

2．管理服务

Windows Server 2003 要管理很多软件和硬件，这些管理大多是通过控制面板来完成的。

Windows Server 2003 控制面板中主要的配置工具有 Internet 选项、存储用户名和密码、打印机和传真、电话和调制解调器选项、电源选项、管理工具和键盘、添加/删除应用程序、添加硬件、授权等，这些和其他 Windows 操作系统使用方法基本上都一样，在这里不再介绍，在这里我们只介绍和网络服务有关系的服务的管理。

1）服务的管理

Windows Server 2003 为用户提供了多种多样的网络服务，如 DHCP 服务、DNS 服务等。可以使用“管理工具”中的“服务”工具对系统的服务器进行管理。操作步骤如下：

（1）双击“管理工具”中的“服务”图标，弹出“服务”窗口，如图 1.29 所示。在窗口

的左部显示的是哪台计算机上的服务，窗口的中部是本地计算机上的服务；窗口的右部是各种不同的服务名称以及服务的描述。也可以选择“操作”→“连接到另一台计算机”命令，对远程计算机上的服务进行管理。

（2）在图 1.29 所示窗口的右部有“扩展”和“标准”两个标签。选择“扩展”标签后，在服务窗口上会显示服务的描述。各种服务功能及其用途可参见服务的描述和以后的章节。

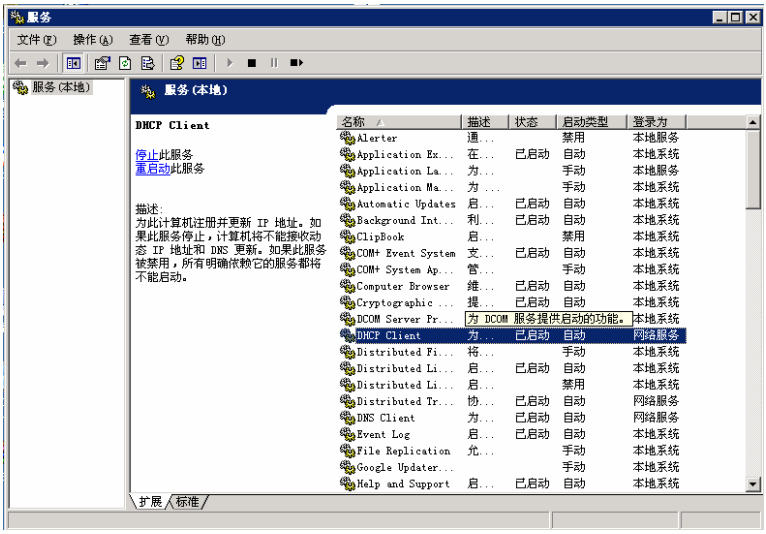

图 1.29 “服务”窗口

（3）要管理某一系统服务，直接双击打开服务的属性窗口。以“DHCP Client”为例，如图 1.30 所示，在“可执行文件的路径”文本框中显示的是为提供服务而执行的文件。“启动类型”下拉列表框中用于显示 Windows Server 2003 系统启动时是否自动启动该服务等；“自动”表示服务随同 Windows 系统的启动而启动；“手动”表示服务不随系统而启动，而是管理员手动启动；“禁止”则是不允许启动该服务。

（4）“服务状态”栏显示的是该服务的状态，可以通过“服务状态”下面的按钮来控制面板的启动、停止等状态。“启动参数”文本框中显示的是启动服务时使用的参数。例如要启动 DNS 服务，如果启动类型为“禁止”，把启动类型改为“手动”后单击“启动”按钮即可。

（5）在服务属性窗口中的“登录”选项卡中，可以设定服务是以登录身份运行的，默认时是“本地系统账户”，如图 1.31 所示。如果要为服务指定登录身份，选择“此账户”单选按钮，然后单击“浏览”按钮打开“选择用户”对话框，选择一个登录用户后单击“确定”按钮，输入账户的密码。

（6）在“登录”选项卡中还可以指定哪个硬件配置文件启动或者禁止该服务。如图 1.31 所示，如果管理员在某一硬件配置文件中禁止了某项服务，则系统启动时如果选择该硬件配置文件，系统将不启动该项服务。

（7）选择“恢复”选项卡，如图 1.32 所示，可以设定服务启动第一次、第二次、后续失败后，系统应采取的相应操作。操作可以是“不操作”、“重新启动服务”、“运行一个程序”和“重新启动计算机”。如果选择“运行一个程序”，还可以选择要运行的程序、命令行参数以及程序在何时启动；如果选择“重新启动计算机”，则可以单击“重新启动计算机选项”按钮打开“重新启动计算机选项”对话框，如图 1.33 所示，可以设置在几分钟后启动计算机以

及是否向管理员发送消息。

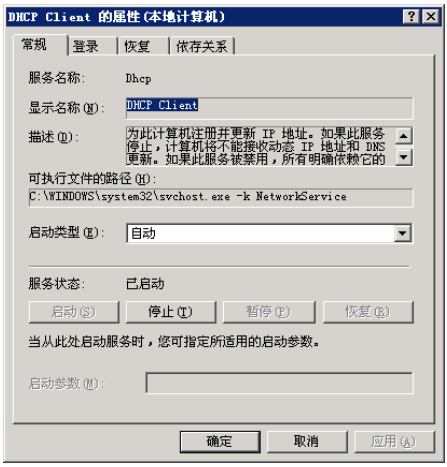

图 1.30 “DHCP 服务属性”对话框

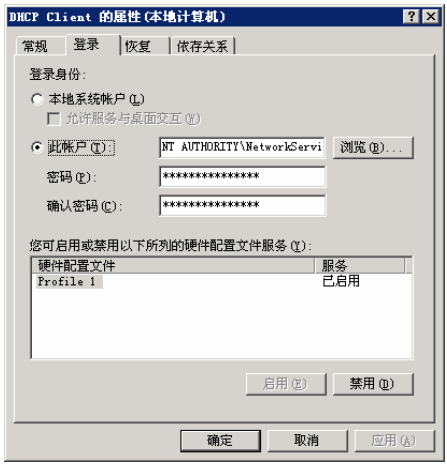

图 1.31 “登录”选项卡

图 1.32 “恢复”选项卡

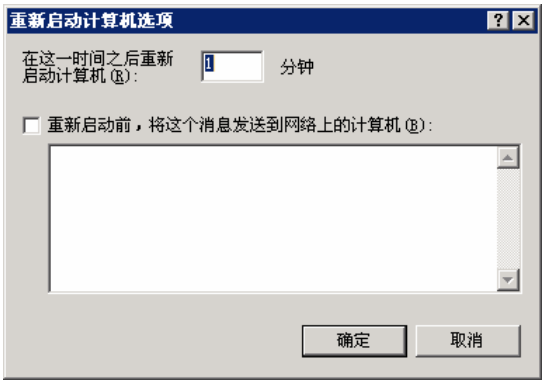

图 1.33 “重新启动计算机选项”对话框

（8）选择“依存关系”选项卡，如图 1.34 所示，可以显示该服务依赖其他哪些服务，以及有哪些服务依赖于它。如果停止某一服务，可能导致依赖于它的其他服务不能正常工作。

2）硬件配置文件

计算机由多种多样的硬件组成，某一时候启用一些硬件而禁用另一些硬件；在另一时候，又需要禁用不同的硬件，在这种情况下可以使用硬件配置文件，硬件配置文件记录了各种硬件设备的资源、驱动程序、启用或禁用的状态等。可以针对每一种工作的需要，建立一个硬件配置文件，当系统启动时选择预先设置好的的硬件配置文件即可。

创建一个硬件配置文件操作步骤如下：

（1）选择“开始→控制面板→系统”命令，打开“系统属性”对话框，选中“硬件”选项卡，单击“硬件配置文件”按钮，弹出“硬件配置文件”对话框，如图 1.35 所示。

（2）在“可用的硬件配置文件”列表框中列出了系统中存在的硬件配置文件，单击“复制”按钮，输入目标配置文件名，单击“确定”按钮即可。

（3）要复制硬件配置文件，选择要被复制的硬件配置文件，单击“复制”按钮，输入目标配置文件名，单击“确定”按钮即可。

（4）有了多个硬件配置文件后，系统在启动时会出现硬件配置文件列表，如图 1.35 所示。

图 1.34　“依存关系”选项卡

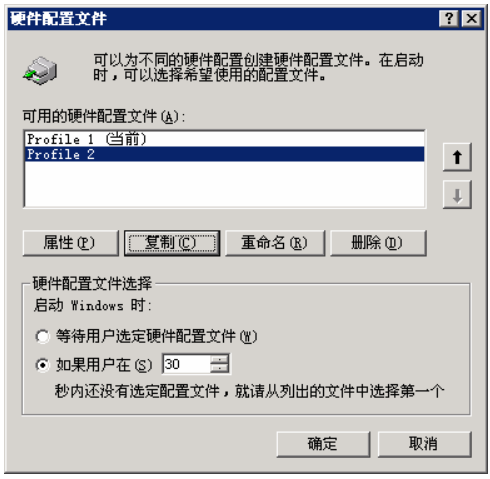

图 1.35　“硬件配置文件”对话框

（5）在如图 1.35 所示的“硬件配置文件”对话框中，在“硬件配置文件选择”选项区域中，可以设定系统等待用户选定硬件配置文件的时间。如果用户没有在设定的时间内选择，系统自动选择第一个硬件配置文件。硬件配置文件的顺序可以通过单击“↑”或者“↓”按钮来改变。

（6）在系统启动时选择某一硬件配置文件后，如果对硬件的设置进行了改动，硬件的设置会保存在当前的硬件配置文件中，不会对其他的硬件配置文件造成影响。

1.5.2　训练 2：TCP/IP协议的设置

服务器只有接入网络才能为其他计算机提供相应的服务，而网卡是计算机与网络连接的唯一接口。因此只有在正确安装网卡驱动程序和网络协议，并正确设置 IP 地址信息之后，服务器才能实现与网络内其他计算机的通信。

1．TCP/IP协议的配置

在 Windows Server 2003 中，只要安装网卡或 MODEM 等网络适配器，系统即可自动安装 Windows Server 2003 默认安装的协议。在 Windows Server 2003 中设置 TCP/IP 协议的步骤如下：

（1）选择“开始→控制面板→网络连接→本地连接”命令，即可打开“本地连接状态”对话框，如图 1.36 所示。在“常规”选项卡中显示了该连接的状态和活动情况，比如这个连接已经建立了 54 分 8 秒，发送了 266 059 个数据包，接收了 518 649 个数据包。“支持”选项卡描述了采用 Internet 协议（TCP/IP）的配置情况，如地址类型（手工配置或自动获取）、实际地址（网卡的 MAC 地址）、IP 地址、子网掩码、默认网关和 DNS 服务器等信息。

（2）单击“属性”按钮，打开“本地连接属性”对话框，如果服务器安装有多块网卡，应当分别选择并一一进行设置。在“此连接使用下列项目”列表框中列出了连接所使用的一些协议、服务等。

（3）在“此连接使用下列项目”列表框中选中“Internet 协议（TCP/IP）”选项，单击“属

性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，如图 1.37 所示。可以选择“自动获取 IP 地址”或用户指定 IP 地址，对于 DNS 服务器也可以选择自动获取或由用户指定。

（4）选中“使用下面的 IP 地址”单选按钮，分别输入为该服务器分配的 IP 地址（在这里输入 10.8.25.178）、子网掩码（在这里输入 255.255.255.0）和默认网关（在这里输入 10.8.25.1），并指定 DNS 服务器的 IP 地址（在这里输入 10.8.10.244）。

图 1.36 “本地连接 状态”对话框

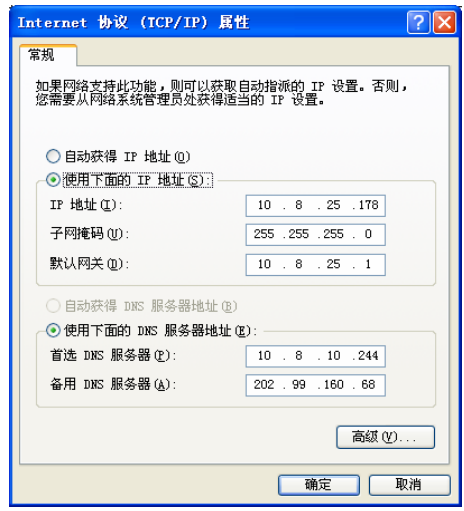

图 1.37 Internet 协议（TCP/IP）属性

（5）单击“确定”按钮，保存所做的修改。

2．TCP/IP协议高级设置

在 Windows Server 2003 中，可以为每块网卡设置多个 IP 地址，在“Internet 协议（TCP/IP）属性”对话框中，单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，单击“IP 地址”框下方的“添加”按钮，弹出“TCP/IP 地址”对话框，如图 1.38 所示，添加 IP 地址（如 IP 地址为 10.8.10.211，子网掩码为 255.255.255.0），添加完后单击“添加”按钮，即可为网卡设置第二个 IP 地址。

图 1.38 为网卡设置多个 IP 地址

3．应用测试命令验证网络连接

（1）在桌面上，选择“开始→运行”命令，打开“运行”对话框，在“打开”文本框中输入 cmd 命令，如图 1.39 所示。单击“确定”按钮，打开“命令提示符”窗口，如图 1.40 所示。

（2）在命令提示符后输入 ipconfig/all 命令，按下 Enter 键，即可查看当前 TCP/IP 的配置信息，如图 1.41 所示。

（3）在命令提示符后输入 ping 10.8.25.101 命令，按下 Enter 键，测试当前计算机和 10.8.25.101 之间的网络是否能够正常通信，如图 1.42 所示。

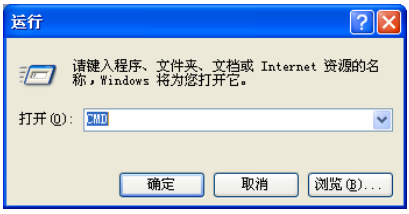

图 1.39　“运行”对话框

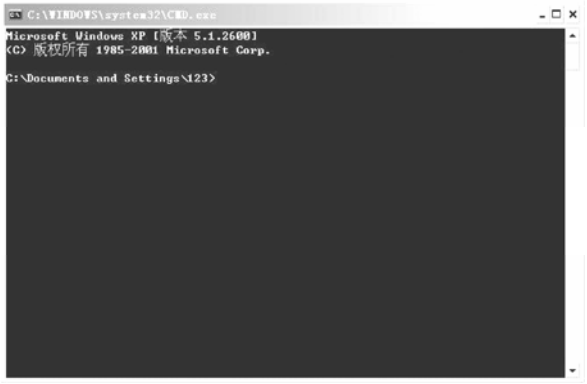

图 1.40　“命令提示符”窗口

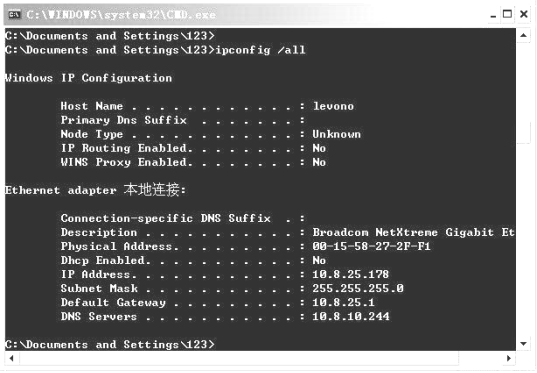

图 1.41　“Ipconfig/all”命令显示结果

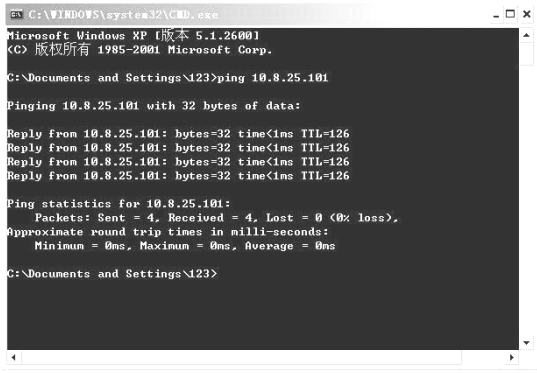

图 1.42　测试网络连接是否正常

1.5.3　训练 3：用户配置文件

在运行 Windows Server 2003 操作系统的计算机上，用户配置文件将自动创建并维护本地计算机上的每个用户工作环境的桌面设置。用户第一次登录到计算机的时侯，系统会为每个独立用户创建一个用户配置文件。这样多个用户可以使用同一台计算机，一个用户对桌面环境的自定义设置不会影响到其他用户的设置。

用户配置文件定义了自定义的桌面环境，包括个人显示设置、网络和打印机连接，以及其他指定的设置。用户或用户的系统管理员可以定义桌面环境。用户配置文件主要有以下几种类型：

（1）本地用户配置文件。第一次登录到计算机时，将创建本地用户配置文件，并存储在计算机的本地硬盘上。对本地用户配置文件所做的任何更改都只是针对用户所在的计算机。

（2）漫游用户配置文件。漫游用户配置文件是一种基于服务器的用户配置文件，会在用户登录时下载到本地计算机，而用户注销时会同时更新本地和服务器的文件。用户登录到工作站或服务器计算机时，服务器的漫游用户配置文件是可用的。登录时如果本地用户配置文件比服务器上的新，则用户可以使用本地用户配置文件。

漫游用户配置文件使用户能够登录到域中的计算机，而同时保留其用户配置文件的设置，存储在由系统管理员指定的服务器位置。

（3）强制用户配置文件。此文件是用来为个人或整个用户组指定特殊设置的漫游配置文件，只有系统管理员才能更改强制用户配置文件。

（4）临时用户配置文件。当错误条件防止加载用户配置文件时会发布临时配置文件，每次会话结束时会删除临时配置文件。当用户注销时，将丢失用户对其桌面设置和文件所做的更改。

1.5.4 训练4：MMC的使用

Windows Server 2003 是一个复杂的系统，要管理好系统需要有各种不同的管理工具，然而管理好这些工具本身就是一件复杂的事情，MMC（Microsoft Manage Console，微软管理控制台）提供了一个管理工具的途径。MMC 允许用户创建、保存并打开管理工具，用来管理硬件、软件和 Windows 的网络组件等。

1．MMC基础

微软管理控制台 3.0（MMC 3.0）是一个框架，它通过提供在不同工具间通用的导航栏、菜单、工具栏和工作流，来统一和简化 Windows 中的日常系统管理任务。使用 MMC 工具（称为管理单元）可以管理网络、计算机、服务、应用程序和其他系统组件。MMC 本身不执行管理功能，但承载了能够执行管理功能的各种 Windows 管理单元和非 Windows 管理单元。

依次单击“开始→运行”，打开“运行”对话框，在该对话框中输入 MMC 命令，可以打开控制台，如图 1.43 所示。

MMC 窗口由两个窗格组成，左边的窗格显示控制台树，控制台树显示控制台中可以使用的项目；右边的窗格是详细信息窗格，详细信息窗格列出了项目的信息和有关功能，详细信息会随着左边的项目不同而不同。

2．添加/删除管理单元

管理单元是 MMC 的基本组件，它总是在控制台中运行，而不能在 MMC 之外运行。MMC 支持两种类型的管理单元：独立管理单元和扩展管理单元。可以独立添加到控制台树中，无须首先添加其他项目的管理单元称为独立管理单元，而需要先添加其他项目才可以被添加的管理单元称为扩展管理单元。

添加管理单元的步骤如下。

（1）在图 1.43 中执行“文件”菜单中的“添加/删除管理单元”命令，弹出“添加/删除管理单元”对话框，如图 1.44 所示。

（2）在“独立”标签中单击“添加”按钮，打开“添加独立管理单元”对话框，如图 1.45 所示，在“可用的独立管理单元”列表框中选择要添加的管理单元后，单击“添加”按钮。添加的管理单元不同，可能会出现新的对话框。

（3）添加完毕后，单击“关闭”按钮，新添加的管理单元将出现在控制台树中。

（4）如果需要添加扩展管理单元，在图 1.44 中选择“扩展”标签，如图 1.46 所示。由于扩展管理单元依赖于独立管理单元，所以要在“可扩展的管理单元”下拉列表框中选择所依附的管理单元，然后选中“添加所有扩展”复选框，或者在“可用的扩展”列表框中选择特定的扩展单元。

（5）选择“文件”菜单中的“保存”或者“另存为”命令可以保存控制台，下次直接双击控制文件打开控制台，原来添加的管理单元将仍旧存在，可以用来进行计算机的管理工作。

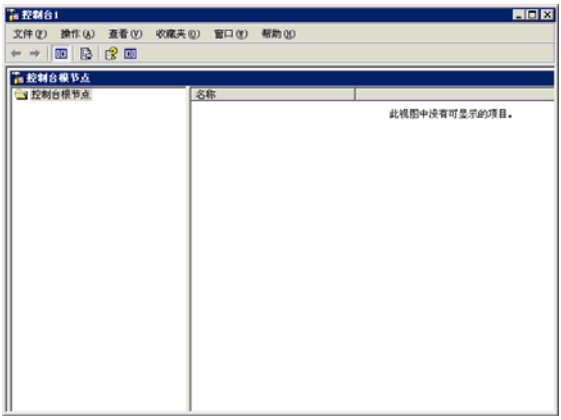

图 1.43 “控制台”窗口

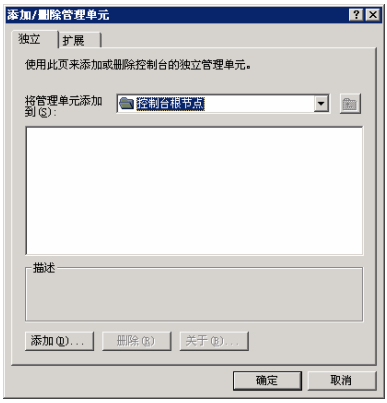

图 1.44 “添加/删除管理单元”对话框

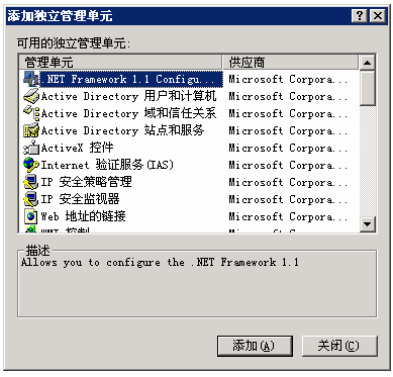

图 1.45 “添加独立管理单元”对话框

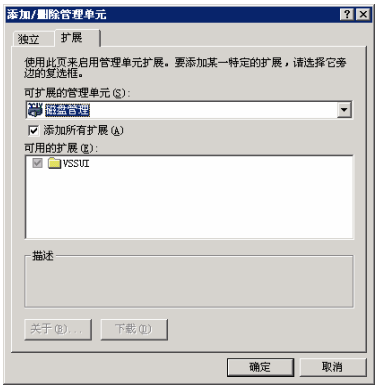

图 1.46 “扩展管理单元”选项卡

3．MMC模式

MMC 有两种模式：作者模式和用户模式。两种模式的访问权限是不一样的。

（1）作者模式。用户既可以向 MMC 添加、删除管理单元，也可以在控制台中创建新的窗口、改变视图等。

（2）用户模式。在用户模式下，有“完全访问”、“受限访问，多窗口”和“受限访问，单窗口”三种访问权限。

完全访问：用户不能添加、删除管理单元或者控制台的属性，但可以访问所有的窗口管理命令，以及所有提供的控制台树的全部权限。

受限访问，多窗口：仅允许用户访问在保存控制台时可见的控制台树的区域，可以创建新的窗口，但是不能关闭已有的窗口。

受限访问，单窗口：仅允许用户访问在保存控制台时可见的控制台树的区域，可以创建新的窗口，阻止用户打开新的窗口。

设置 MMC 模式的步骤如下。

（1）在图 1.43 中，执行“文件”菜单中的“选项”命令，弹出“选项”对话框，如图 1.47 所示。

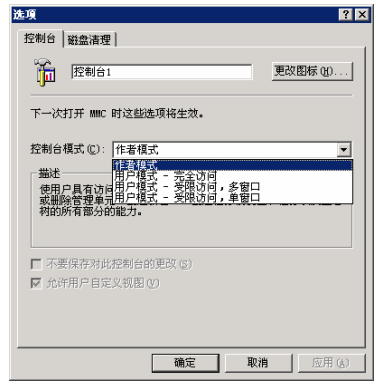

图 1.47 “选项”对话框

（2）单击“更改图标”按钮可以选择一个新的图标文件，在“控制台模式”下拉列表框中选择所要设定的模式。

（3）选中“不要保存更改到此控制台”复选框，用户更改控制台后，关闭控制台时不会把更改保存在控制台文件中。

（4）“允许用户自定义视图”复选框用于控制用户能否从“查看”菜单中自定义控制台右边窗格的视图。

习　题

一、填空题

1．Windows Server 2003 有四个版本，分别为_____、_____、_____和_____。

2．推荐将 Windows Server 2003 安装在_____文件系统内。

3．系统管理员的用户名为_____。

4．无人值守安装的命令格式为_____。

5．使用_____可以自动产生无人值守安装的应答文件。

6．为提高 Windows Server 2003 系统的安全性，在系统启动时必须按_____组合键，输入正确密码后才能登录。

二、选择题

1．下面哪一个工具可以自动产生无人值守安装的应答文件？（　　）

A．deploy.cab　　B．setupmgr.exe

C．sysprep.exe　　D．winnt32.exe

2．某企业规划有两台 Windows Server 2003 和 50 台 Windows XP，每台服务器最多只有 15 人能同时访问，最好采用哪种授权模式？（　　）

A．每服务器模式　　B．每客户模式

C．域模式　　D．集中管理模式

3．推荐将 Windows Server 2003 安装在（　　）文件系统分区上。

A．NTFS　　B．FAT　　C．FAT32　　D．VFat

4．Windows Server 2003 支持下面哪些文件系统格式？（　　）

A．NTFS　　B．FAT　　C．FAT32　　D．EXT3

5．Windows Server 2003 的安装方式包括（　　）。

A．全新安装　　B．升级安装

C．远程服务器安装　　D．无人值守安装

三、思考题

1．Windows Server 2003 有哪些版本，它们的用途分别是什么？

2．硬盘分区的作用是什么？

3．NTFS 文件系统和 FAT32 文件系统有何区别？

四、实训题

1．从光盘安装 Windows Server 2003，设置相应的信息，包括，计算机名为 xpc-xxgcx-server1，IP 地址

为 192.168.1.100，子网掩码为 255.255.255.0，默认网关为 192.168.1.1，DNS 为 202.99.16.68，系统管理员密码为 qazWSXedc123456，授权模式为每服务器模式，用户数为 200 个。

2．修改安装光盘的 I386 目录下的 unattend.txt 文件，应答信息参见训练项目 1 的要求。

3．用安装管理器产生无人值守安装的应答文件，应答信息参见训练项目 1 的要求。

4．使用 ipconfig 命令查看 IP 地址信息，使用 ping 命令测试网络连通性。

项目 2　工作组模式下的用户、组和文件管理

2.1　项目内容

1．项目目的

通过在工作组模式下对 Windows Server 2003 服务器进行配置和管理，掌握用户、组的管理，理解 NTFS 和 FAT32 文件系统的区别，理解文件和文件夹权限与共享权限的区别，了解本地安全策略，理解工作组的概念以及工作组模式的应用。

2．项目任务

有一家小型公司，组建了单位的局域网，采用 Windows Server 2003 操作系统，现需要根据公司人员身份的不同创建不同的用户账户，这些账户根据身份不同可使用的计算机不同，可访问的文件及文件夹的权限不同。

3．任务目标

① 学会在 Windows Server 2003 中创建用户账户；
② 学会在 Windows Server 2003 中创建组账户；
③ 掌握在 Windows Server 2003 中为用户账户分配权限；
④ 掌握在 Windows Server 2003 中创建共享并使用共享。

2.2　相关知识

2.2.1　Windows Server 2003 的工作模式

根据网络中计算机的配置和访问信息的方式，网络可分为两种类型：对等式网络（peer-to-peer）和客户/服务器网络（Client/Server）。

1．对等式网络

如图 2.1 所示，对等式网络（常常被称为对等网）中资源是分布存放在各台计算机中的，网络中没有专用的服务器。图 2.1 中的主机 A～E 都有文件要共享出去给其他主机使用。在主机 A 共享资源给主机 B、C、D、E 时，A 就是服务器，主机 B、C、D、E 就是客户机。同样，如果主机 A 使用主机 B 共享出去的资源，主机 A 就是客户机，主机 B 就是服务器。每台计算机同时是服务器和客户机。在 Windows Server 2003 网络中，这种网络类型就是工作组模型。

由于资源是分布存放的，所以对资源的管理也是分布进行的。在图 2.1 中，需要每台主机上的用户各自管理自己主机上的资源。这样对用户的要求就较高，同时也容易造成管理上的混乱。对等式网络安装比较容易，不需要专门的服务器和专门的网络管理人员，成本也比较低。适用于计算机数量小于 15 台的小型网络，如家庭或小型办公网络。

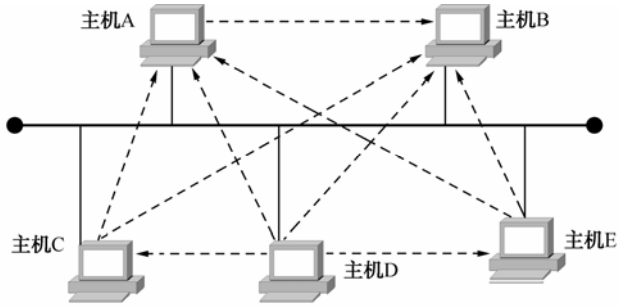

图 2.1　对等式网络

2．客户/服务器网络

当网络规模大到一定程度时，对等式网络的管理工作量就会大到无法接受的程度，这时应该采用客户/服务器网络，也称为主从式网络，如图 2.2 所示。在客户/服务器网络中，有专门的服务器提供服务，充当服务器角色；其余的计算机则是客户机；客户/服务器网络中，资源集中存放在服务器上，网络管理主要集中在服务器上进行，管理相对容易。客户/服务器网络比较适用于较大的网络，对服务器的硬件要求较高，也需要专门的网络管理员，成本较高。

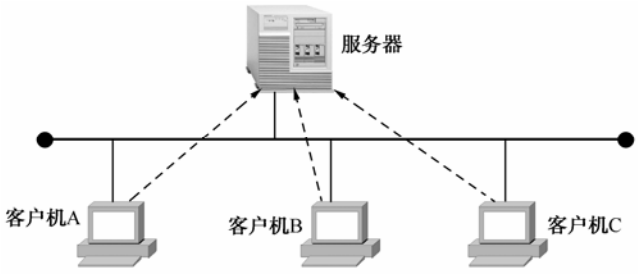

图 2.2　客户/服务器网络

2.2.2　用户账户

1．账户的命名

在计算机网络中，计算机的服务对象是用户，用户通过账户访问计算机资源，所以用户也是账户。所谓用户的管理就是账户的管理。

Windows Server 2003 通过建立账户并赋予账户合适的权限来保证使用网络和计算机资源的合法性，以确保数据访问、存储和交换服从安全需要。

用户账户是计算机的基本安全组件，计算机通过用户账户来辨别用户身份，让有使用权限的人登录计算机，访问本地计算机资源或从网络访问这台计算机的共享资源。用户账号是用来记录用户的用户名和口令、隶属的组、可以访问的网络资源以及用户的个人文件和设置。赋予不同用户不同的权限，可以让用户执行不同的计算机管理任务。所以每台运行 Windows Server 2003 的计算机，都需要用户账户才能登录计算机。在登录过程中，Windows Server 2003 要求用户指定或输入不同的用户名和密码，当计算机比较用户输入的账户与密码与本地安全数据库中的用户信息一致时，才能让用户登录到本地计算机或从网络上获取对资源的访问权限。用户登录时，本地计算机验证用户账户的合法性，如用户提供了正确的用户名和密码，则本地计算机分配给用户一个访问令牌，该令牌定义了用户在本地计算机上的访问权限，资

源所在的计算机负责对该令牌进行鉴别，以保证用户只能在管理员定义的权限范围内使用本地计算机上的资源。对访问令牌的分配和鉴别是由本地计算机的本地安全权限（LSA）负责的。

在 Windows Server 2003 系统中，系统会为每一个用户账户建立一个唯一的安全标识码（Security Identifier，SID），Windows Server 2003 系统都是利用这个 SID 来代表该用户，有关的权限设置等都是通过 SID 来设置的，而不是利用用户的账户名称。

SID 不会被重复使用，即使将某个账户删除后，再添加一个相同名称的账户，它也不会拥有原来账户的权限，因为它们的 SID 不同，对 Windows Server 2003 系统而言，它们是不同的账户。

用户通过账户名和密码来标识。

1）命名约定

- 账户名必须唯一：本地账户必须在本地计算机上唯一。
- 账户名不能包含以下字符：*/ \ [ ] ☹ = ， + < > ”。
- 账户名最长不能超过 20 个字符，由数字和字符组成，输入时可超过 20 个字符，但只识别前 20 个字符。
- 不能与用户组的组名相同。

2）密码原则

① 一定要给每一个用户账户指定一个密码，尤其是 administrator 账户，以防止他人随便使用该账户。

② 不要包含使用者账户名称的全部或任何部分。

③ 要包含下列四种字符中的三种：

- 英文大写字符（A～Z）；
- 英文小写字符（a～z）；
- 10 进位数字（0～9）；
- 非英文字母字符（如!、$、#、%）、扩充型 ASCII、符号或语音字符。

④ 密码最多可由 128 个字符组成，推荐最小长度为 8 个字符。

2．账户的类型

Windows Server 2003 有两种工作模式：工作组模式和域模式。针对这两种工作模式，也有两种用户身份：域用户和本地用户。在本项目中只介绍本地用户账户。

1）域用户账号

域用户账号建立在域控制器的 Active Directory 数据库内。用户可以利用域用户账号来登录域，并利用它来访问网络上的资源，例如访问其他计算机的文件、打印机等资源。

当用户利用域用户账号登录时，由域控制器检查用户所输入的账号与密码是否正确。

将用户账号建立在某台域控制器内后，该账号会自动复制到同一域内的其他所有域控制器中。因此，当该用户登录时，此域内的所有域控制器都可以负责审核用户的身份，即检查用户所输入的用户名与口令是否正确。

2）本地用户账号

本地用户账号建立在 Windows Server 2003 独立服务器的本地安全数据库内，而不是域控制器内。用户可以利用本地用户账号来登录此计算机，但是只能够访问这台计算机内的资源，

无法访问网络上的资源。

本地用户账号只存在于这台计算机内，Windows Server 2003 不会将其复制到域控制器的活动目录内。

当用户利用本地用户账号登录时，这台计算机将根据本地安全数据库来检查账号与密码是否正确。

在此建议用户最好不要在 Windows Server 2003 成员服务器或已加入域的 Windows Server 2003 内建立本地用户账号，因为无法访问域上的资源，同时域系统管理员也无法管理这些本地用户账号。因此，域结构的网络中用户的账号最好都建立在域控制器的活动目录内。

3）内建用户账号

在安装 Windows Server 2003 时一并安装的用户账号称为内建用户账号，通常为 Administrator 和 Guest。

（1）Administrator：该账号为初次安装 Windows Server 2003 系统后的预设系统管理员，因此具有“至高无上”的权力。它可对整个域或计算机进行设置，例如：用户账号与组的建立、更改、删除，建立打印机、设置安全策略、设置用户账号的权限、分配资源等。该账号可以更名但无法删除，也无法禁止。因此，为了安全起见，进入系统后应将 Administrator 账号更名。

（2）Guest：该账号用来提供给来宾作为临时账号使用，所谓来宾就是偶尔要求登录入网的用户，该账号具有少部分的权限。Guest 账号可以被更名，但无法删除它，要使用该账号时，首先要设置它为允许（Enable）使用，缺省设置它为禁止（Disable）。

Guest 账号用于在该计算机所在的域或者受该计算机所在域委托的任何域上都没有实际账号的人。账号禁用（但未被删除）的用户也能使用 Guest 账号。Guest 账号不需要密码，而且有两种类型登录：本地来宾登录和网络来宾登录。你可以配置每个域和计算机，使其允许两种、一种或者不允许任何一种类型登录。安装 Windows Server 2003 后，在默认情况下 Guest 账号被禁用，但可将其设置为有效。

2.2.3 组账户

组是 Windows Server 2003 中对用户账户的一种逻辑单位，是将具有相同特点和属性的用户组合成一个组，其目的是方便管理和使用。组账户是计算机的基本安全组件，是用户账户的集合，但是组账户并不能用于登录计算机。通过使用组，管理员可以同时向一组用户分配权限。同一个用户账户可以同时为多个组的成员。

Windows Server 2003 独立服务器上的组又称为本地组。Windows Server 2003 内置本地组主要包括 Administrators、Backup operators、Guests、Power users、Print operators、Remote desktop users、Users 等。

打开“计算机管理”控制台，在“本地用户和组”树中的“组”目录里，可以查看本地内置的所有组账户。

Windows Server 2003 内置的组账户的权限见表 2.1。

表 2.1　Windows Server 2003 内置组账户的权限

组	描　　述	默认用户权限
Administrators	其成员具有对服务器的完全控制权限，并且可以根据需要向用户指派用户权利和权限，默认成员有 Administrator 账户	从网络访问此计算机；允许本地登录；调整某个进程的内存配额；允许通过终端服务登录；备份文件和目录；更改系统时间；调试程序；从远程系统强制关机；加载和卸载设备驱动程序；管理审核安全日志；调整系统性能；关闭系统；取得文件或其他对象的所有权
Backup operators	其成员可以备份和还原服务器上的文件，而不考虑保护这些文件的安全设置	从网络访问此计算机；允许本地登录；备份文件和目录；忽略遍历检查；还原文件和目录；关闭系统
Guests	其成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾账户（默认禁用）也是该组的成员	没有默认用户权限
Network configuration operators	其成员可以更改 TCP/IP 设置，并更新和发布 TCP/IP 地址。无默认成员	没有默认用户权限
Performance monitor users	其成员可以在本地服务器和远程客户端查看性能计数器，并不需要是 Administrators 或 Performance monitor users 的成员	没有默认用户权限
Performance log users	其成员可以在本地服务器和远程客户端管理性能计数器、日志和警报，而不需要成为 Administrators 的成员	没有默认用户权限
Power users	其成员可以创建用户账户，然后修改并删除所有所创建的账户。可以创建本地组，然后在已创建的本地组中添加或删除用户，还可以在 Power users 组、Users 组和 Guests 组添加后删除用户。可以创建共享资源并管理所创建的共享资源。但是不能取得文件的所有权、备份或还原目录、加载或卸载设备驱动程序，或者管理安全性及日志	从网络访问此计算机；允许本地登录；忽略遍历检查；更改系统时间；调整单一进程；关闭系统
Print operators	其成员可以管理打印机打印队列	没有默认用户权限
Remote desktop users	其成员可以远程登录服务器	允许通过终端服务登录
Users	其成员可以执行一些常见任务，包括运行应用程序、使用本地和网络打印机以及锁定服务器等。不能共享目录或创建本地打印机。在本地创建的任何用户账户，都可以成为本组的成员	从网络访问此计算机；允许本地登录；忽略遍历检查

计算机上所有本地账户和组账户的安全信息都存储在用户数据库 SAM（Security Accounts Managers，安全账户管理器）中。SAM 数据库的文件路径是“%windir%\system32\config\sam”。如果该文件被删除，则本地计算机所有账户信息都会丢失，Administrator 账户的密码将被置为空。

2.2.4 NTFS文件系统及NTFS权限

1．NTFS文件系统

NTFS（New Technology File System）文件系统是一个基于安全性的文件系统，它是建立在保护文件和目录数据基础上，同时照顾节省存储资源、减少磁盘占用量的一种先进的文件系统。Windows Server 2003 采用的 NTFS 文件系统是 NTFS 5.0。

NTFS5.0 的特点主要有：

① 支持分区的容量可以达到 2TB。如果是 FAT32 文件系统，支持分区的容量最大为 32GB；

② 是一个可恢复的文件系统。NTFS 通过使用标准的事务处理日志和恢复技术来保证分区的一致性；

③ 支持对分区、文件夹和文件的压缩；

④ 采用了更小的簇，可以更有效地管理磁盘空间；

⑤ 在 NTFS 分区上，可以为共享资源、文件夹以及文件设置访问许可权限；

⑥ 在 Windows Server 2003 的 NTFS 文件系统下可以进行磁盘配额管理；

⑦ NTFS 使用一个“变更”日志来跟踪记录文件所发生的变更。

而 FAT32 文件系统只能设置共享方式的访问权限，而没有文件和文件夹的访问权限。NTFS 文件系统拥有更高的安全性，不仅可以设置共享方式的访问权限，还可以设置文件和文件夹的访问权限，因此应该优先选用 NTFS 文件系统。

2．NTFS权限类型

Windows Server 2003 在 NTFS 磁盘上提供了 NTFS 权限。利用 NTFS 权限，系统管理员或文件拥有者可以指定特定用户和组访问某个文件或文件夹的权限，以此来允许或禁止用户和组对文件或文件夹的操作，实现对数据资源的保护。

在 NTFS 文件系统中，每个文件和文件夹都建立了一个访问控制列表（ACL），其中列出了不同用户和组对该文件或文件夹所拥有的访问权限。当用户访问该资源时，系统首先查看 ACL，检查用户是否有足够的权限完成他所请求的操作。

只有在 NTFS 格式的磁盘可以设置 NTFS 权限，FAT16 和 FAT32 格式的磁盘上不能使用 NTFS 权限。

NTFS 权限可以针对所有的文件、文件夹、注册表键值、打印机和动态目录对象进行权限的设置。在 NT4.0（Windows NT 使用）许可中包括的内容有完全控制、修改、读并且执行、读和写，称为普通权限。

1）文件夹的 NTFS 权限

选择一个文件夹，右击选择“属性”命令，再选择“安全”选项卡，如图 2.3 所示。

- 完全控制：用户可以修改、增加、移动或删除文件及其属性和目录。用户能够修改所有文件和子目录的权限设置。
- 修改：用户可以查看并修改文件或者文件属性，包括在目录下增加或删除文件，以及修改文件属性。
- 读取和执行：用户可以运行可执行文件，包括脚本。
- 列出文件夹目录：可以浏览文件夹及其子文件夹的目录内容，但不具有在该文件夹内建立子文件夹的权利。

- 读取：用户可以查看文件和文件属性。
- 写入：用户可以对一个文件进行写操作。

在新的 NTFS5.0（Windows 2000/XP/2003）中，微软对这些权限进行了升级，在普通权限的基础上进行了加强，称为特殊权限。例如，在特殊 NTFS 权限中把标准权限中的“读取”权限分为“读取数据”、“读取属性”、“读取扩展属性”和“读取权限”四种更加具体的权限。在图 2.3 所示的对话框中单击“高级”按钮，然后在弹出的“高级安全设置”对话框中选择一个用户账户单击“编辑”按钮，即可设置特殊的 NTFS 权限，如图 2.4 所示。

图 2.3 “文件夹属性”对话框

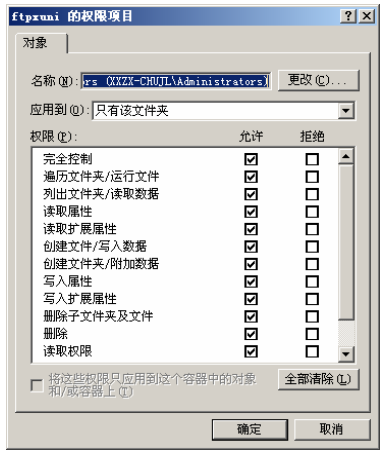

图 2.4 特殊权限选择

下面就来介绍这些特殊 NTFS 权限的功能。

（1）遍历文件夹/运行文件：“遍历文件夹”可以让用户即使在无权访问某个文件夹的情况下，仍然可以切换到该文件夹内。这个权限设置只适用于文件夹，不适用于文件。只有当组或用户在“组策略”中没有赋予“绕过遍历检查”用户权限时，对文件夹的遍历才会生效。在默认情况下，everyone 组具有“绕过遍历检查”的用户权限，所以此处的“遍历文件夹”权限设置不起作用。“运行文件”让用户可以运行程序文件，该权限设置只适用于文件，不适用于文件夹。

（2）列出文件夹/读取数据：“列出文件夹”让用户可以查看该文件夹内的文件名称与子文件夹的名称。“读取数据”让用户可以查看文件内的的数据。

（3）读取属性：该权限让用户可以查看文件夹或文件的属性，如只读、隐藏等属性。

（4）读取扩展属性：该权限让用户可以查看文件夹或文件的扩展属性。扩展属性是由应用程序自行定义的，不同的应用程序可能有不同的设置。

（5）创建文件/写入数据：“创建文件”让用户可以在文件夹内创建文件；“写入数据”让用户能够更改文件内的数据。

（6）创建文件夹/附加数据：“创建文件夹”让用户可以在文件夹内创建子文件夹；“附加数据”让用户可以在文件的后面添加数据，但是无法更改、删除、覆盖原有的数据。

（7）写入属性：该权限让用户可以更改文件夹或文件的属性，如只读、隐藏等属性。

（8）写入扩展属性：该权限让用户可以更改文件夹或文件的扩展属性。扩展属性是由应用程序自行定义的，不同的应用程序可能有不同的设置。

（9）删除子文件夹及文件：该权限让用户可以删除该文件夹内的子文件夹与文件，即使用户对这个子文件夹或文件没有“删除”的权限，也可以将其删除。

（10）删除：该权限让用户可以删除该文件夹与文件。即使用户对该文件夹或文件没有“删除”的权限，但是只要他对其父文件夹具有“删除子文件夹及文件”的权限，他还是可以删除该文件夹或文件。

（11）读取权限：该权限让用户可以读取文件夹或文件的权限设置。

（12）更改权限：该权限让用户可以更改文件夹或文件的权限设置。

（13）取得所有权：该权限让用户可以夺取文件夹或文件的所有权。文件夹或文件的所有者，无论对该文件夹或文件权限是什么，永远具有更改该文件夹或文件权限的能力。

2）文件的 NTFS 权限

应用在文件上的 NTFS 权限来控制用户对文件的访问。下面列出了文件所具有的 NTFS 权限类型。

- 读取：允许查看文件内容、所有者、属性和权限。
- 写入：改写文件、更改文件属性及查看所有权和权限。
- 读取和运行：具有“读取”权限，并可以运行应用程序。
- 修改：包括“写入”以及“读取和运行”权限，允许修改、删除文件。
- 完全控制：运行全部的权限，可以获得文件的所有权。

3．NTFS权限的设置

NTFS 权限设置就是指定特定用户和组对某个文件或文件夹的访问权限。只有文件或文件夹的所有者、系统管理员或者具有“完全控制”权限的用户才可以设置文件或文件夹的 NTFS 权限。

4．对象的所有权

Windows 中任何一个对象都有所有者，所有者与其他权限是彻底分开的。对象的所有者拥有一项特殊的能力——更改对象的权限设置。

在默认情况下，创建文件和文件夹的用户是该文件和文件夹的所有者，拥有对象的所有权。除了用户自行新建的对象外，Windows Server 2003 中其他对象的所有者都是本地 Administrator 组的成员。

Administrator 组的成员可以取得系统中任意对象的所有权，这是操作系统为了管理的需要，而给予管理员组成员的特权。

5．NTFS权限的规则

NTFS 权限设置是一项复杂而细致的工作。用户账户可能属于多个组，每个组可能对同一对象有不同权限；用户对父文件夹和子文件夹的权限要求可能不尽相同；用户可能通过其他途径得到他不应该拥有的权限。网络中 70%的安全问题都是因为管理员操作不当造成的。下面是 NTFS 权限的几个重要规则，在设置权限时，一定要全面考虑，注意用户最终的有效权限是什么，避免由于不恰当设置造成安全隐患。

1）NTFS 权限的继承规则

① 子文件夹和文件默认继承父文件夹的权限；

② 用户继承其所属组的权限，并且这种权限是累加的。

2）文件权限优先于文件夹权限规则

虽然文件总是位于文件夹内，但是文件的 NTFS 权限设置优先级要高于文件夹的 NTFS 权限设置。如果在文件夹中的某个文件上设置了用户有访问的权限，即使用户对文件夹没有

访问的权限，用户也可以使用文件的物理路径来直接访问文件。

3）拒绝权限优先于允许权限规则

出于安全考虑，NTFS 权限规定拒绝权限优先于允许权限。例如，对于用户“Xiaosbygl1”，是“everyone”组的成员，具有“读”的权限，但他是“tempemp”组的成员，还有“拒绝”的权限，那么“拒绝”权限的优先级最高。

4）NTFS 权限的应用规则

（1）同级权限的组合。当一个用户属于多个用户组时，就会出现同级权限组合的情况，例如，对于计算机“财务部 2”的“cwwd3”这个共享资源，用户“caiwbjl”在通过远程访问时，既是“everyone”组的成员，又是“manager”组的成员，以前者的身份，他只有“读”的权限，以后者的身份，他有“完全控制”的权限，那么他的权限就是两者权限的最大组合，即有“完全控制”的权限。

同级权限的组合原则是：同级权限的组合取最大权限，但拒绝权限优先级最高。

（2）不同级权限的组合。当用户通过共享方式访问另一台计算机上的资源时，可能会出现既有文件和文件夹权限设置，同时又有共享权限设置的情况，这时的原则是：不同级权限的组合取最小权限。

由此可以得出结论：同级权限的组合取最大权限，不同级权限的组合取最小权限，拒绝权限优先级最高。

5）移动和复制操作对权限操作的影响

（1）在同一个分区内移动文件或文件夹时，此文件和文件夹会保留在原位置的一切 NTFS 权限；在不同的 NTFS 分区之间移动文件或文件夹时，文件或文件夹会继承目的分区中文件夹的权限。

（2）在同一个分区内复制文件或文件夹时，文件和文件夹会继承目的位置中的文件夹的 NTFS 权限；在不同的 NTFS 分区之间复制文件或文件夹时，文件或文件夹将继承目的位置中文件夹的权限。

（3）从 NTFS 分区向 FAT 分区中复制或移动文件和文件夹，都将导致文件和文件夹的权限丢失。

2.2.5 Windows Server 2003 资源共享

在网络环境中，管理员和用户除了可以使用本地资源外，还可以使用其他计算机上的资源。在资源使用的过程中，对于用户来说，不需要知道资源的位置；而对于共享资源来说，也不需要知道用户的位置，双方都是透明的，用户只要了解到网络中有自己所需要的资源，并且有资源的使用权限，就可以使用该资源。从这个意义上来说，同一个资源可以被多个用户使用，因此称为“资源共享”。

利用共享文件夹来进行共享的资源主要是指计算机的软件资源，计算机的软件资源是指程序和数据，在网络中表现为文件夹和文件，软件资源的共享实质上是文件和文件夹的共享。

1．共享权限

共享权限只有三种：读取、更改和完全控制。Windows Server 2003 默认的共享文件设置权限是 everyone，即用户具有读取权限。而 Windows Server 2000 默认的共享文件设置权限是 everyone，即用户具有完全控制权限。

- 读取：读取权限是指派给 everyone 组的默认权限。可以查看文件名和子文件夹名；查看文件中的数据；运行程序文件。
- 更改：更改权限不是任何组的默认权限。更改权限除允许所有的读取权限外，还增加添加文件和子文件夹、更改文件中的数据、删除子文件夹和文件等权限。
- 完全控制：是指派给本机上的 Administrators 组的默认权限。完全控制权限除允许全部读取权限外，还具有更改权限。

2．共享文件夹的访问权限

1）复制和移动对共享权限的影响

当共享文件夹被复制到另一位置后，原文件夹的共享状态不会受到影响，复制产生的新文件夹不会具备原有的共享设置。

当共享文件夹被移动到另一位置后，原文件夹将失去原有的共享设置。

2）共享权限和 NTFS 权限

共享权限仅对网络访问有效，当用户从本机访问一个文件夹时，共享权限完全派不上用场。NTFS 权限对网络访问和本地访问都有效，但是要求文件或文件夹必须在 NTFS 分区上，否则无法设置 NTFS 权限。

当一个共享文件夹设置了共享权限和 NTFS 权限后，就要受到两种权限的控制：

如果希望用户能够完全控制共享文件夹，首先要在共享权限中添加此用户（组），并设置完全控制权限，然后在 NTFS 权限设置中添加此用户（组），并设置完全控制权限。只有两个地方都设置了完全控制权限，才能最终拥有完全控制权限。

当用户从网络访问一个存储在 NTFS 文件系统上的共享文件夹时，会受到两种权限的约束，而有效权限是最严格的权限（也就是两种权限的交集）。当用户从本地计算机直接访问文件夹的时候，不受共享权限的约束，只受 NTFS 权限的约束。

例如，共享权限为只读，NTFS 权限为写入，那么最终权限是完全拒绝。

2.3　方案设计及准备

1．设计

为了完成项目任务，设计一个小型网络，拥有 3 台计算机，这 3 台计算机组成一个基于工作组的小型网络，现在需要对这些计算机进行配置，应满足下列要求：

（1）公司内有 5 位员工，需要使用这些计算机，每位用户的部门，用户账户初始密码等信息，见表 2.2。

表 2.2　用户账户

部　门	用户账户名称	用 户 全 名	描　述	初 始 密 码
销售部	Xiaosbjl	张三	销售部经理	Xiaosbjl
销售部	Xiaosbyg1	李四	销售部员工	Xiaosbyg1
财务部	Caiwbjl	王五	财务部经理	Caiwbjl
财务部	Caiwbyg1	马六	财务部员工	Caiwbyg1
销售部	Xiaosbygl1	赵七	销售部员工（临时）	Xiaosbygl1

（2）销售部有一台计算机，由销售部的 3 位员工共用，财务部有两台计算机，由财务部的两位员工各自使用。每台计算机都有本部门的共享目录，设置合适的目录访问权限，见表 2.3。

表 2.3　共享资源的权限分配

计　算　机	使　用　人	文 件 夹 名	共享目录名	文件夹权限	共 享 权 限
销售部 1	销售部全体员工	xiaoswd	xswd		全体员工拥有读写权限
		Xiaosht		销售部经理拥有读写权限，其他员工不可访问	不共享
财务部 1	王五	Cwwd1	Cwwd1		财务部员工拥有读权限
财务部 2	马六	Cwwd2	Cwwd2		财务部员工拥有读写权限；销售部员工拥有读权限
		Cwwd3	Cwwd3		部门经理拥有完全权限；全体员工拥有读权限；临时工没有任何权限

（3）根据以上要求，本项目实施的网络拓扑结构如图 2.5 所示。

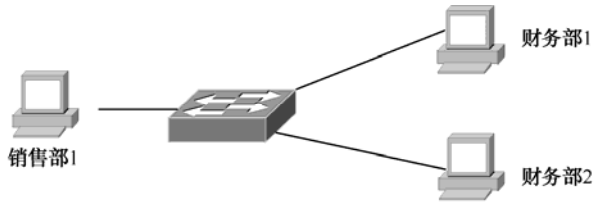

图 2.5　网络拓扑图

2．设备清单

为了搭建图 2.5 所示的网络环境，需要如下设备：

① PC 3 台，安装有 Windows Server 2003 操作系统，作为独立服务器，每台计算机的磁盘中有 NTFS 和 FAT32 文件系统的分区；

② 交换机 1 台；

③ 直通线 3 条。

2.4　项目实施

步骤 1：硬件安装

按照图 2.5 所示用 3 条直通线将 3 台计算机连接到交换机上，检查网卡和交换机的指示灯的连接状态，判断网络是否连通。

步骤 2：TCP/IP配置

（1）配置财务部 1 的 IP 地址为 192.168.1.10，子网掩码为 255.255.255.0；配置财务部 2 的 IP 地址为 192.168.1.20，子网掩码为 255.255.255.0；配置销售部 1 的 IP 地址为 192.168.1.30，子网掩码为 255.255.255.0。

（2）财务部 1、财务部 2 和销售部 1 之间通过 ping 命令检查网络的连通性。

步骤 3：更改计算机名

为组内的 3 台计算机分别设置计算机名称：销售部 1、财务部 1、财务部 2。

（1）右击“我的电脑”，在弹出的快捷菜单中选择“属性”选项，打开“系统属性”对话框，选中“计算机名”选项卡，如图 2.6 所示。

（2）单击“更改”按钮，打开“计算机名称更改”对话框，如图 2.7 所示。在“计算机名”文本框中输入计算机名称，如销售部 1。

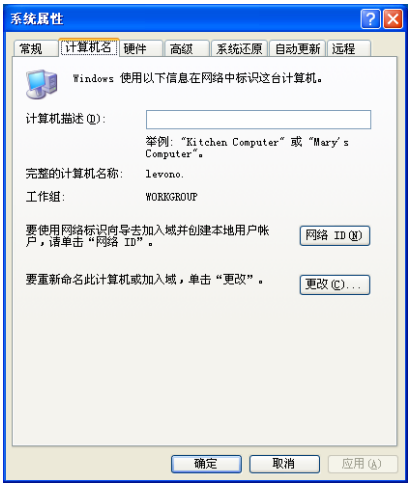

图 2.6 “系统属性”窗口

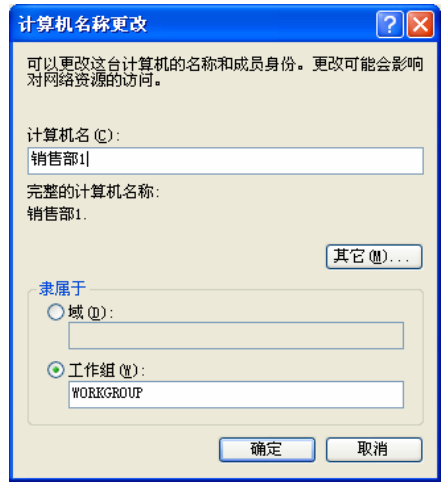

图 2.7 “计算机名称更改”对话框

（3）单击“确定”按钮，返回到“系统属性”窗口，再次单击“确定”按钮，系统会要求重新启动设置才能生效。

步骤 4：创建本地用户账户

以创建用户账户 Xiaosbjl 为例来介绍创建的过程。

（1）以 Administrator 身份登录。建立本地账户可以用“计算机管理”中的“本地用户和组”管理单元来创建本地用户账户，而且必须拥有管理员权限。

（2）选择“开始→管理工具→计算机管理”选项，弹出“计算机管理”窗口，依次展开“系统管理→本地用户和组→用户”，在“计算机管理”窗口右侧列出已经存在的账户，如图 2.8 所示。

（3）右击“用户”，从弹出的菜单中选择“新用户”命令，弹出“新用户”对话框，如图 2.9 所示。输入用户名、全名、描述和密码。为了避免在输入时被他人看到密码，因此在对话框中的密码只会以星号（*）显示。需要再次输入密码来确认所输入的密码是否正确。密码最多 128 个字符，密码的大小写是有区别的。

可以设置密码选项，包括以下四种。

- “用户下次登录时需更改密码”：强迫用户在下次登录时必须更改密码。该项设置可以确保只有该用户知道该密码。
- “用户不能更改密码”：它可以防止用户更改密码，如果多人共享一个账户时（例如 Guest），则选择此复选框，避免发生被某个人更改密码后，造成其他人都无法登录的情况。
- “密码永不过期”：若选择此复选框，则系统永远不会要求该用户更改密码，即使在

“账户策略”的“密码最长存留期”中设置了所有用户必须定期更改密码，系统也不会要求这个用户更改密码。

- “账户已停用”：禁止用户利用此账户登录。一般用于新账户暂时不生效或员工离职时。

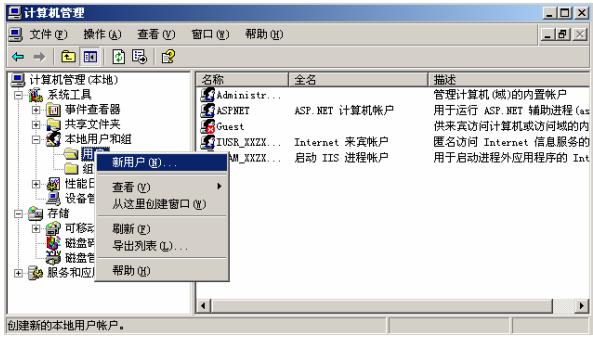

图 2.8 “计算机管理”窗口

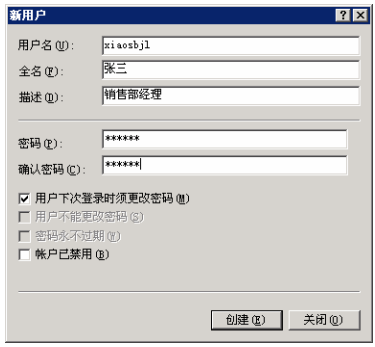

图 2.9 “新用户”对话框

（4）设置完成后，单击“创建”按钮新增用户账户。创建完用户后，单击“关闭”按钮返回“计算机管理”控制台。

按照表 2.4 的要求分别在 3 台计算机上创建新用户，同一员工可能需要在不只一台计算机上创建用户。

表 2.4 用户的创建

计 算 机 名	使 用 者	远 程 访 问 者	需 要 的 用 户
销售部 1	销售部共用	全体员工	张三、李四、王五、马六、赵七
财务部 1	王五	财务部员工	王五、马六
财务部 2	马六	全体员工	张三、李四、王五、马六、赵七

（5）设置用户账户的属性

打开“计算机管理→系统工具→本地用户和组→用户”窗口，双击一个用户（鼠标右击一个用户选择属性），弹出“用户属性”对话框，如图 2.10 所示。

① “常规”选项卡。可以设置与账户有关的一些描述信息，如全名、描述、账户选项等。

② “隶属于”选项卡。选择“隶属于”选项卡，打开“隶属于”选项对话框，可以设置将该账户加入其他的本地组中。单击“添加”按钮，弹出“选择组”对话框，用户可以直接输入组的名称，如管理员组的名称“Administerators”。输入组名称后，若需要检查名称是否正确，则单击“检查名称”按钮，名称会变为“xxzx-chujl\administrators”，前面部分表示本地计算机名称，后面部分为组名称，如图 2.10 所示。

如果不希望手动输入组名称，也可以选择单击“高级”按钮，再单击“立即查找”按钮，从列表中选择一个或多个组。

③ “配置文件”选项卡。选择“配置文件”选项，打开配置文件选项对话框，可以设置用户账户的配置文件路径、登录脚本和主文件夹路径，如图 2.11 所示。

图 2.10　给用户账户选择组

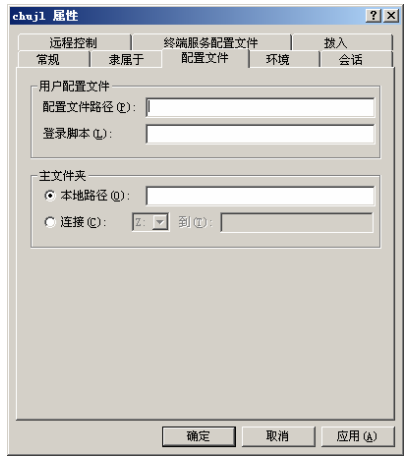

图 2.11　“配置文件”选项卡

- 用户配置文件是存储当前桌面环境、应用程序设置以及个人数据的文件夹和数据的集合，还包括所有登录到某台计算机上所建立的网络连接。
- 当用户第一次登录到某台计算机上时，Windows Server 2003 自动创建一个用户配置文件并将其保存在该计算机上。
- 配置文件路径：本地用户账户的配置文件保存在本地磁盘%userprodile%文件夹中。
- 登录脚本：登录脚本是希望用户登录计算机时自动运行的脚本文件，脚本文件的扩展名可以是 VBS、BAT 和 CMD。
- 主文件夹：Windows Server 2003 为每个用户提供了用于存放个人文档的主文件夹。

（6）删除用户账户。当用户不再需要使用某个用户账户时，可以将其删除。删除用户账户会导致与该账户有关的所有信息的遗失。

在“计算机管理”控制台中，选择要删除的用户账户，右击选择“删除”即可。但系统内置账户（Administrator 和 Guest）无法删除。

步骤 5：创建组账户

通常情况下，系统默认的用户组已经能够满足需要，但有时不能满足特殊安全和灵活性的需要，管理员需要新增一些组。这些组创建以后，就可以像内置组一样，赋予其权限和进行组成员的增加。

以在计算机销售部 1 上创建组 sales 为例来介绍组的创建和用户的加入。

（1）选择“开始→管理工具→计算机管理”命令，弹出“计算机管理”窗口，依次展开“系统管理→本地用户和组→组”，在“计算机管理”窗口右侧列出已经存在的本地组。

（2）右击“组”，选择“新建组”选项，弹出“新建组”对话框。在“组名”框中输入新组的名称，如 sales，在“描述”框中输入新组的说明，如销售部所有员工，如图 2.12 所示。

（3）要向新组添加一个或多个成员，在“新建组”对话框中单击“添加”按钮，弹出“选择用户”对话框，如图 2.13 所示。

（4）此时可以在“输入对象名称来选择”栏下手工直接输入用户账户名称，如管理员的

名称“Administerator”。输入用户账户（或组）后，若需要检查名称是否正确，则单击“检查名称”按钮，名称会变为“xxzx-chujl\administrator”。前面部分表示本地计算机名称，后面部分为用户账户（或组）名称。

如果不希望手动输入用户账户（或组）名称，也可以选择单击“高级”按钮，窗口展开，如图 2.14 所示。再单击“立即查找”按钮，系统会自动搜索在“查找位置”中的所有用户，选择用户“xiaosbjl”，如图 2.15 所示，单击“确定”按钮。返回“新建组”对话框，刚才添加的用户账户已经添加到了成员栏中。

图 2.12　“新建组”对话框

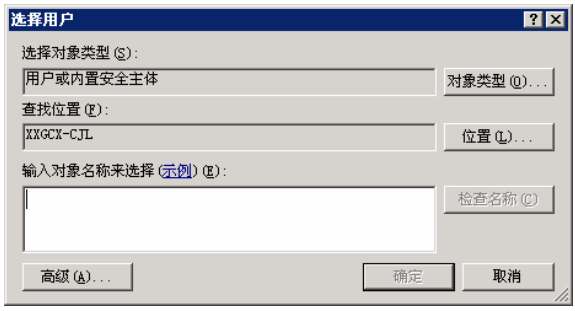

图 2.13　“选择用户”对话框

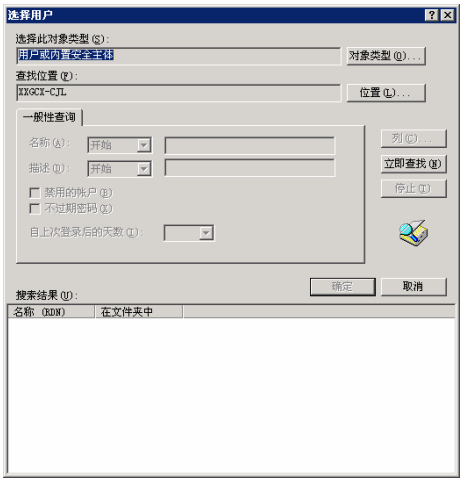

图 2.14　高级选择用户

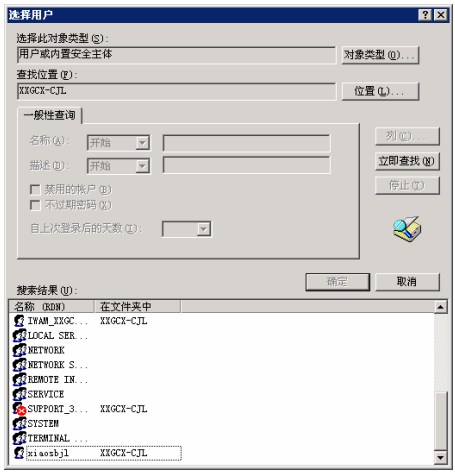

图 2.15　搜索用户

（5）单击“创建”和“关闭”按钮，即可完成创建。按照表 2.5 的要求分别在 3 台计算机上创建组，并将用户加入到组中。每台计算机上的组是各自独立的，只能将本地计算机上的用户加入其中。

表 2.5　组的创建

计 算 机 名	组　　名	成　　员
销售部 1	Sales	销售部全体员工
财务部 1	Sales	销售部全体员工
	Financial	财务部全体员工
财务部 2	Manager	各部门经理
	Tempemp	临时工，赵七

（6）删除、重命名本地组及修改本地组。当计算机中的组不需要时，系统管理员可以对组执行清除任务。每个组都拥有一个唯一的安全标识符（SID），所以，一旦删除了用户组，就不能重新恢复，即使新建一个与被删除组有相同名字和成员的组，也不会与被删除组有相同的特性和权限。在“计算机管理”控制台选择要删除的组账户，然后执行删除功能。

但是管理员只能删除新增的组，不能删除系统内置的组。

在“计算机管理”控制台选择要重命名的组账户，然后执行重命名功能。

要修改本地组成员，只要双击组名称，弹出“组属性”对话框，如图 2.16 所示。选择成员单击“删除”按钮即可删除组成员。如果要添加组成员，单击“添加”按钮，再选择相应用户即可。

图 2.16　“组属性”对话框

步骤 6：设置本地安全策略

根据项目要求需要在财务部的两台计算机上设置本地安全策略。密码策略设置“密码长度最小值”为 7，强制密码历史为 5，其他为默认值。账户锁定策略设置“账户锁定阈值”为 3，修改“账户锁定时间”为 20 分钟，修改“复位账户锁定计数器”为 30 分钟。

（1）选择“开始→管理工具→本地安全策略”命令，打开“本地安全设置”窗口，展开“账户策略→密码策略”，在“本地安全设置”窗口右侧列出密码策略，如图 2.17 所示。

（2）设置“密码长度最小值”为 7，双击“密码长度最小值”，打开“密码长度最小值属性”对话框，如图 2.18 所示，在“密码必须至少是”栏中设置数值 7，单击“应用”按钮，单击“确定”按钮，返回“本地安全设置”对话框，此时密码长度最小值已更改为 7。

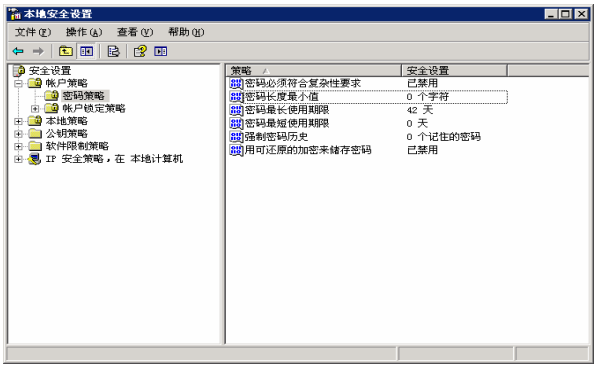

图 2.17　“本地安全设置”窗口

图 2.18　密码长度最小值属性

（3）设置“强制密码历史”为 7，双击“强制密码历史”，打开“强制密码历史属性”对话框，如图 2.19 所示，在“保留密码历史”栏中设置数值 5，单击“应用”按钮，单击“确定”按钮，返回“本地安全设置”对话框，此时已更改为 5。

其他保留默认值，其中密码最长使用期限为 42 天，表示在有效期结束之前，用户必须更换新的密码，并且新的密码不能与以前最近使用过的 5 个密码相同。

（4）单击“账户锁定策略”，在右侧显示账户锁定策略，如图 2.20 所示，双击“账户锁

定阈值”，打开“账户锁定阈值属性”对话框，如图 2.21 所示，在“在发生以下情况之后，锁定账户”设置“3 次无效登录”。单击“应用”按钮，打开“建议的数值改动”窗口，如图 2.22 所示。显示“账户锁定时间”为 30 分钟，“复位账户锁定计数器”为 30 分钟，单击“确定”按钮返回“本地安全设置”对话框。此时“账户锁定时间”为 30 分钟，“复位账户锁定计数器”为 30 分钟。双击“账户锁定时间”更改时间为 20 分钟。使用该设置后，如果某用户登录失败的次数达到 3 次，该用户将被锁定，无法登录，直到管理员手工为该用户解除锁定，或者等待 20 分钟的锁定时间，系统自动为其解锁。

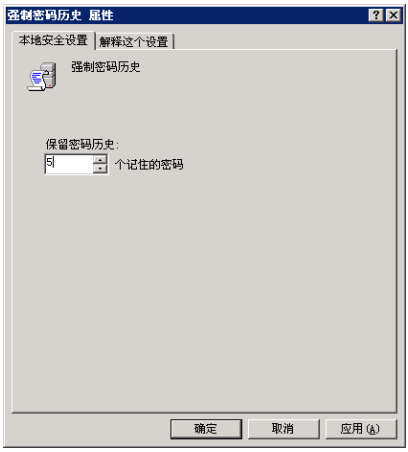

图 2.19　“强制密码历史属性”对话框

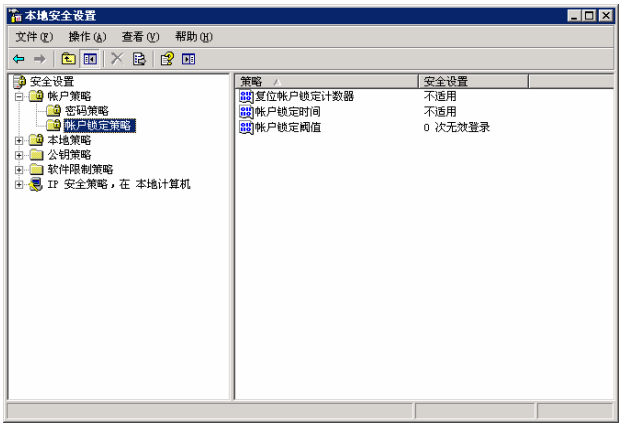

图 2.20　“账户锁定策略”窗口

图 2.21　“账户锁定阈值属性”对话框

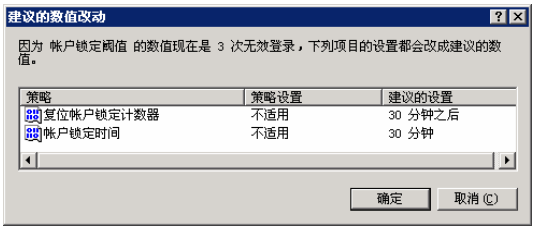

图 2.22　“建议的数值改动”窗口

步骤 7：新用户账户使用

（1）注销当前 Administrator 用户，以新建的用户账户（例如 Xiaosbjl）登录，登录后系统提示修改密码。对于财务部的计算机，如果新密码长度小于 7 个字符，系统会拒绝接受。

（2）用户登录后，可随时修改自己的密码，按下 Ctrl+Alt+Del 组合键，然后选择“修改密码”。

在财务部的计算机上设置的密码策略将防止用户设置与原来相同的密码。

同一用户在不同计算机上都有账户，这些账户是独立的，因此修改密码应该在 3 台计算

机上改成统一的密码。

管理员可以更改其他用户的密码。以 Administrator 用户身份登录，依次选择“开始→管理工具→计算机管理”命令，弹出“计算机管理”窗口，依次展开“系统管理→本地用户和组→用户”，在“计算机管理”窗口右侧列出已经存在的账户，选择需要更改密码用户，右击鼠标，在菜单中选择“设置密码”选项，弹出“警示信息”，单击“继续”按钮，弹出“为用户设置密码”对话框，如图 2.23 所示。在“新密码”和“确认密码”栏中输入相同的密码，单击“确定”按钮，完成用户密码更改。

（3）测试账户锁定。在财务部的计算机上测试账户锁定，注销当前用户，以新建的用户账户登录，故意输入错误的密码 3 次，这时该账户被系统锁定，无法登录。

Administrator 管理员账户不会被锁定，即使多次输入错误的密码。管理员可以手工解除锁定，首先以管理员身份登录，选择被锁定的用户，右击鼠标，选择“属性”，打开用户属性对话框，如图 2.24 所示。在“常规”选项卡下，将“账户已禁用”多选框的选择取消。

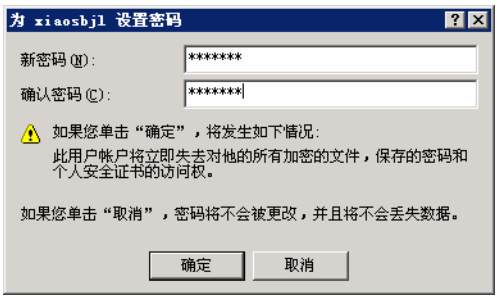

图 2.23 “为用户设置密码”对话框

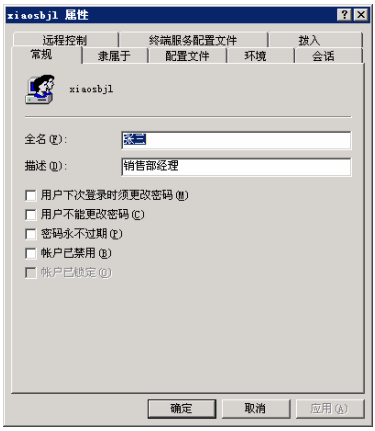

图 2.24 用户属性对话框

步骤 8：设置文件夹权限

对于重要的资源应该设置访问权限。例如在计算机“销售部 1”，该计算机可以由销售部的所有员工共用，文件夹“xsht”只能由销售部经理访问，其他员工即使从本机登录也不能访问。为实现该目的，需要按如下步骤操作。

（1）以管理员身份登录，在“资源管理器”中，在 D 盘创建 xsht 文件夹，选择该文件夹右击鼠标，选择“属性”命令，打开“xsht 属性”对话框，单击“安全”选项卡（如果该文件夹在 FAT32 文件系统中，则没有“安全”选项，无法继续），如图 2.25 所示。

（2）单击“添加”按钮，打开“选择用户或组”对话框，选择用户“xiaosbjl”，如图 2.26 所示。单击“确定”按钮，再次单击“确定”按钮，返回文件夹“xsht 属性”对话框，设置“xiaosbjl”的权限为“完全控制”，如图 2.27 所示。

（3）为防止其他用户的访问，必须删除“Users”组的权限。Users 组是一个内置组，所有新建的用户都将自动成为该组的成员，因此，其他用户将可以通过 Users 组的授权而访问“xsht”文件夹。该组的权限是通过继承得来的，因此从“组或用户名称”列表中删除“Users”之前，必须先取消该目录的继承权限选项。选中“Users”组，单击“高级”按钮，打开“xsht 的高级安全设置”对话框，如图 2.28 所示，清除“允许父项的继承权限传播到该对象和所有

子对象，包括那些在此明确定义的项目”选项的选择，打开“安全”对话框，选择“复制或删除”。取消继承权限后即可从“组或用户名称”列表中删除“Users”组。

图 2.25 “xsht 属性”对话框

图 2.26 “选择用户或组”对话框

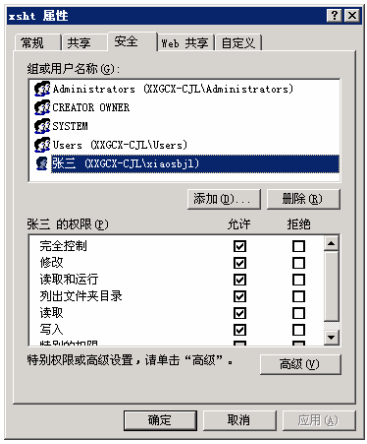

图 2.27 设置权限

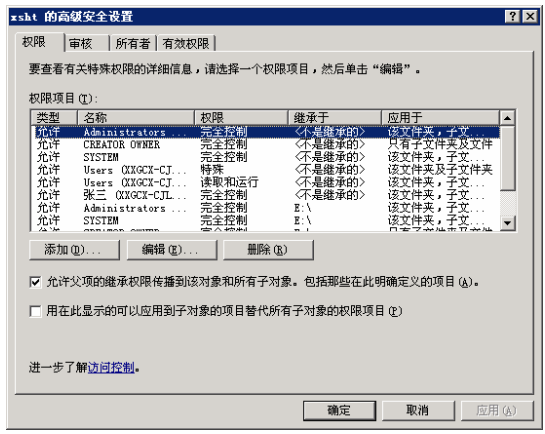

图 2.28 高级安全设置

（4）权限设置完成，注销当前用户，分别以“xiaosbj1”、“xiaosbyg1”身份登录，可以发现前者有权访问“xsht”文件夹，而后者无法访问。

步骤 9：设置共享权限

在 Windows Server 2003 网络中，并非所有用户都可以设置文件夹共享。首先，具备文件夹共享的用户必须是 Administrator、Server Operator、Power Users 等内置组的成员；其次，如果该文件夹位于 NTFS 分区，该用户必须对被设置的文件夹具备“读取”的 NTFS 权限。如果用户希望服务器上的程序和数据能被网络上的其他用户所使用，必须创建共享文件夹。在“我的电脑”和“资源管理器”窗口中，用户可随时创建共享文件夹。

（1）利用“共享文件夹向导”创建共享文件夹。在 Windows Server 2003 中，可以通过“共享文件夹向导”设置共享文件夹。

① 选择“开始→管理工具→计算机管理”命令。弹出“计算机管理”窗口，展开“共享文件夹”，在窗口的右边显示出了计算机中所有共享文件夹的信息。右击“共享”选项，选

择“新建文件共享”选项，弹出“共享文件夹向导”对话框，如图 2.29 所示。在“文件夹路径”栏中输入要共享的文件夹路径。

图 2.29　“共享文件夹向导”对话框

② 单击“下一步”按钮，弹出“名称、描述和设置”对话框，设置共享名和描述，如图 2.30 所示。

③ 单击“下一步”按钮，弹出“权限”对话框，用户可以根据自己的需要设置网络用户的访问权限。或者选择“自定义”来定义网络用户的访问权限。

④ 单击“完成”按钮完成共享文件夹的设置。

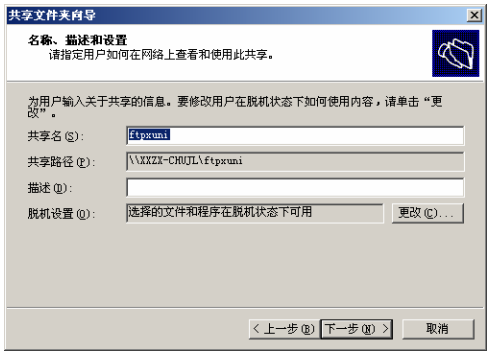

图 2.30　“名称、描述和设置”对话框

（2）在“我的电脑”或“资源管理器”中创建共享文件夹。下面以计算机“销售部 1”中的“xswd”文件夹为例，介绍设置共享的操作步骤。

① 以管理员身份登录，在“资源管理器”中，在 D 盘创建 xswd 文件夹，选择该文件夹，右击，选择“属性”命令，打开“xswd 属性”对话框，单击“共享”选项卡，如图 2.31 所示。选中“共享此文件夹”选项，可以进行如下的设置：

- 共享名和描述：可以将“共享名”设置为希望的共享名称，共享名默认为文件夹名，即为 xswd，并在“描述”部分为该共享文件夹进行简单的注释加以说明。
- 用户数限制：在默认状态下，并不限制通过网络同时访问共享文件夹的用户数量，即设置为“最多用户”，根据需要可以选择“允许的用户数量”单选按钮，并在其后设置具体数值加以限制。

② 单击“权限”按钮，打开“xswd 的权限”对话框，如图 2.32 所示。设置 everyone 的权限，默认只有“读取”权限，设置 everyone 具有“完全控制”权限。

③ 以同样的方式在计算机“财务部 1”和“财务部 2”上设置共享文件夹，其共享权限见表 2.6。

④ 设置完成后用不同的身份登录测试。

⑤ 管理共享文件夹。

可以通过“计算机管理”工具来管理所有的共享。图 2.33 所示为本机“销售部 1”上的所有共享的文件夹，其中前面几个是 Windows 默认设置的，共享名后的符号“$”将会隐藏

共享，使该共享在“网上邻居”中不可见。从“会话”中可以监视当前哪些用户从哪台计算机访问共享；从“打开文件”中可以监视当前哪些文件被哪个用户访问，以及访问的类型（读或写）。在“共享”中也可以新建共享，在“会话”中也可以中断正在进行中的共享连接，在“打开文件”中也可以关闭打开的文件。

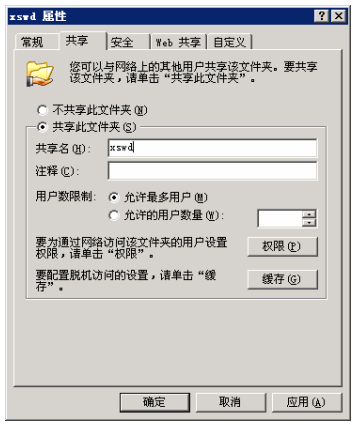

图 2.31　“xswd 属性”对话框

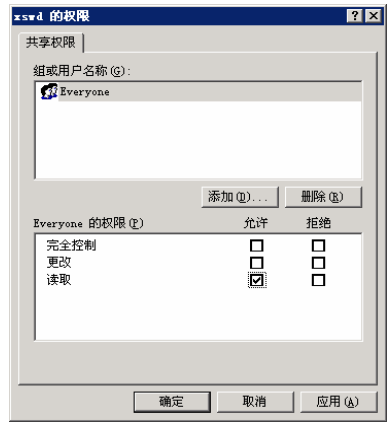

图 2.32　“xswd 的权限”对话框

表 2.6　共享权限设置

计 算 机 名	共享文件夹	用 户 或 组	身　份	完 全 控 制	更　改	读　取
销售部 1	xswd	Everyone	所有用户		允许	允许
财务部 1	Cwwd1	Everyone	从列表中删除			
		Financial	财务部			允许
财务部 2	Cwwd2	everyone	从列表中删除			
		Financial	财务部		允许	允许
		Sales	销售部			允许
	Cwwd3	everyone	所有用户			允许
		Manager	部门经理	允许	允许	允许
		Tempemp	临时人员	拒绝	拒绝	允许

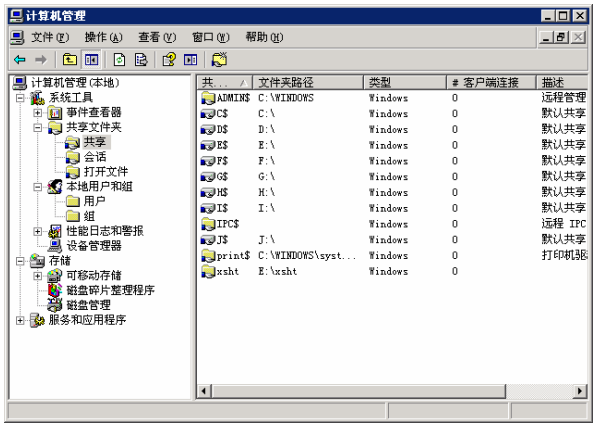

图 2.33　“计算机管理”窗口

步骤 10：禁止从本机登录

用户“赵七”需要通过远程访问计算机“财务部 2”上的“Cwwd3”共享资源，因此，在计算机“财务部 2”上存在“赵七”这个账户，这是很不安全的，需要禁止该用户在该计算机上登录，从而避免其直接访问该计算机。

（1）在计算机“财务部 2”上，以管理员身份登录。

（2）依次选择“开始→管理工具→本地安全策略”命令，打开“本地安全设置”窗口，展开“本地策略→用户权限分配”，在“本地安全设置”窗口右侧列出用户权限分配的策略，如图 2.34 所示。

（3）设置“拒绝本地登录”。双击“拒绝本地登录”，打开“拒绝本地登录属性”对话框，如图 2.35 所示。单击“添加用户或组”添加拒绝本地登录的用户或组。在此名单中的用户或组将不能在计算机“财务部 2”上通过本地登录的方式访问，但仍然可以通过共享方式访问计算机“财务部 2”上的资源。

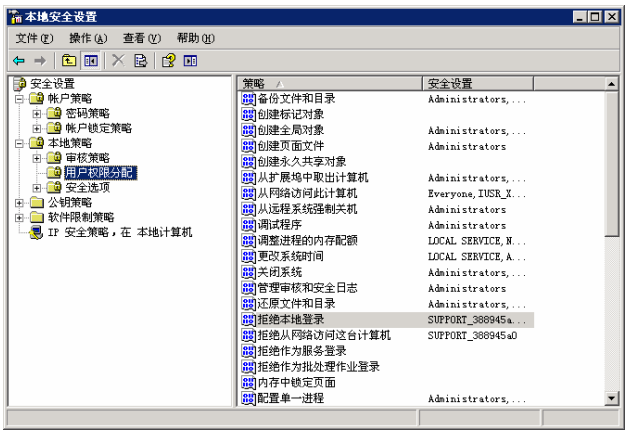

图 2.34 “本地安全设置”窗口

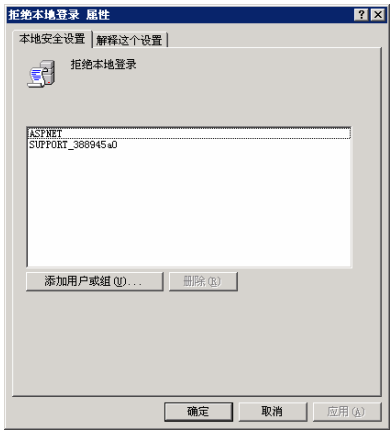

图 2.35 “拒绝本地登录属性”对话框

步骤 11：访问共享文件夹

当用户知道网络中某台计算机上有需要的共享信息后，就可在自己的计算机上使用这些资源。在 Windows Server 2003 中，提供了多种快速访问网络资源的方式。下面介绍三种访问共享文件夹的方法。

（1）搜索计算机。当用户要访问某个计算机时，如果知道该计算机的名称或 IP 地址，可直接利用“搜索计算机”功能在整个网络中进行搜索。

① 在“网上邻居”窗口中或 Windows Server 2003 桌面上，右击“网上邻居”，选择“搜索计算机”选项，如图 2.36 所示，打开“搜索结果—计算机”窗口，在“您在查找哪台计算机”文本框中输入要搜索的计算机名称或 IP 地址。输入完后，单击“搜索”按钮，系统会将搜索到的计算机列在窗口右边的列表框中，如图 2.37 所示。

② 搜索到计算机后并双击，即可访问该计算机上的共享资源。

（2）建立网上共享文件夹的直接链接。在 Windows Server 2003 中，允许用户建立与共享资源的直接链接，以便实现对共享资源的快速访问。

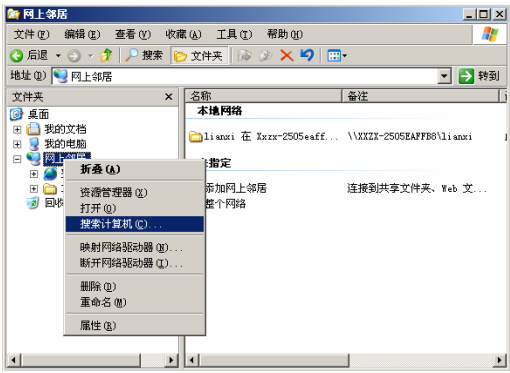

图 2.36 “网上邻居”窗口

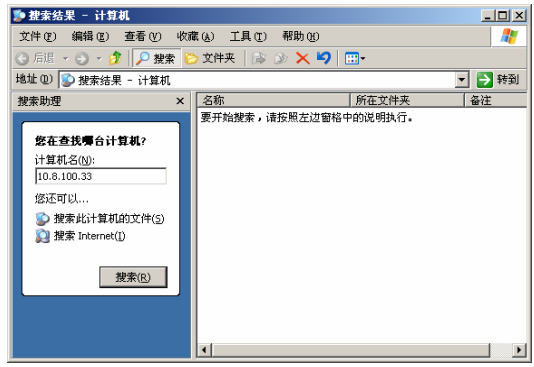

图 2.37 “搜索结果—计算机”窗口

① 在“网上邻居”窗口中，双击“添加网上邻居”图标，弹出“欢迎使用添加网上邻居向导”对话框，根据向导提示，单击“下一步”按钮，直到出现如图 2.38 所示的对话框。

② 在“Internet 或网络地址”下拉列表框中，直接输入该计算机的完整名称，也可通过单击“浏览”按钮，打开“浏览网络资源”对话框，从中选择一个服务器（共享文件夹所在的计算机），单击“确定”按钮退出。

③ 单击“下一步”按钮，弹出如图 2.39 所示的对话框，输入这个网上邻居的名称。

图 2.38 填写 Internet 或网络地址

图 2.39 为网上邻居命名

④ 单击“下一步”按钮，再单击“完成”按钮即可创建共享文件夹的直接链接，随后，共享文件夹图标就出现在“网上邻居”窗口中。

（3）映射网络驱动器。如果用户在网上共享资源时，需要频繁访问网上的某个共享文件，则可以为他设置一个逻辑驱动器号——网络驱动器。网络驱动器设置好后，就会出现在“我的电脑”窗口和“资源管理器”中，双击网络驱动器的图标，即可直接访问该驱动器下的文件或文件夹。

① 在“网上邻居”窗口中，找到需要映射网络驱动器的文件夹。

② 右击该共享文件夹，选择“映射网络驱动器”选项，弹出“映射网络驱动器”对话框，如图 2.40 所示。打开“我的电脑”窗口，执行“工具”菜单下的“映射网络驱动器”选项，也可打开“映射网络驱动器”对话框。

③ 在“驱动器”下拉列表框中选择一种要显示的驱动器符号。在默认情况下，Windows

XP 和 Windows Server 2003 将映射网络驱动器分配给高可用驱动器号，开头驱动器为 Z，以避免驱动器号冲突。

④ 在“文件夹”下拉列表框中通过“浏览”按钮查找共享文件夹，也可直接输入共享文件夹，格式为\\server\share。

⑤ 单击“完成”按钮，就可映射网络驱动器。被映射的网络驱动器将出现在“Windows 资源管理器”的“我的电脑”中。在“我的电脑”窗口中双击代表该共享文件夹的网络驱动器的图标，即可直接访问该驱动器下的文件和文件夹。

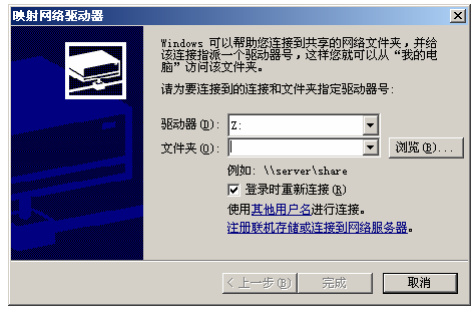

图 2.40 “映射网络驱动器”对话框

⑥ 需要断开网络驱动器时，只需选择“Windows 资源管理器”中的“工具”菜单下的“断开网络驱动器”，然后选择要断开连接的网络驱动器，并单击“确定”按钮即可。

也可使用 net 命令映射网络驱动器。将共享文件夹映射到特定驱动器号，在 netuse 命令中指定驱动器号或驱动器号映射网络驱动器窗口中单击。例如，将\\server\share 映射到驱动器 G，在命令提示符下输入以下命令：

```
netuse g: \\server\share
```

习 题

一、填空题

1．拥有_____是用户登录到网络并使用网络资源的基础。

2．系统管理员的用户名是_____。

3．管理员可以通过_____的方法，来管理其他用户创建的文件夹或文件。

二、选择题

1．在安装 Windows Server 2003 的服务器上，下面哪个用户账户有重新启动服务器的权限？（　　）

A．Guest　　B．User　　C．Admin　　D．Administator

2．为了保护系统安全，下面哪个账户应该被禁用？（　　）

A．Guest　　B．Annonymous　　C．User　　D．Administator

3．本地用户和组的信息存储在“%windir%\system32\config”文件夹的（　　）文件中。

A．SAM　　B．data　　C．user　　D．ntds.dit

4．本地计算机上使用管理工具中的（　　）工具来管理本地用户和组。

A．系统管理　　B．计算机管理　　C．服务　　D．数据源

5．公司某员工出国学习 3 个月，这时管理员最好是将该员工的用户账户（　　）。

A．删除　　B．禁用　　C．关闭　　D．不需作处理

6．在 NTFS 文件系统的分区中，对一个文件夹的 NTFS 权限进行如下的设置；先设置为读取、后设置为写入、再设置为完全控制，则最后，该文件夹的权限类型是（　　）。

A．读取　　B．写入　　C．读取和写入　　D．完全控制

7．使用（　　）可以将 FAT32 格式的分区转化为 NTFS 分区，且用户的文件不受损害。

A．change.exe　　B．convert.exe　　C．cmd.exe　　D．config.exe

8．某 NTFS 分区上有一个文件夹 A1，其中有一个文件“file1.doc”和一个应用程序“notepad. exe”。A1 的 NTFS 安全选项中仅设置了用户组 G1 具有读取权限，用户组 G2 具有写入权限。某用户 user1 同时属于 G1 和 G2，则下面说法不正确的是（　　）。

A．user1 可以运行程序 notepad.exe　　B．user1 可以打开文件 file1

C．user1 可以修改文件 file1 的内容　　D．user1 可以在 A1 中创建子文件夹

9．某 NTFS 分区上有一个文件夹 A1，其中有一个文件“file1.doc”。A1 的 NTFS 权限中仅设置了用户组 G1 具有读取权限；A1 的共享权限中设置用户组 G1 具有完全控制权限。当某用户 user1 在局域网中通过网上邻居访问文件夹 A1 时，下面说法正确的是（　　）。

A．user1 可以删除文件 file1　　B．user1 不能打开文件 file1

C．user1 不能重命名 file1　　D．user1 可以修改文件 file1 的内容

三、思考题

1．文件夹的 NTFS 权限有哪些？

2．文件的 NTFS 权限有哪些？

3．共享文件夹的权限有几种类型？

4．如何隐藏磁盘的分区共享？

5．复制和移动对共享权限有什么影响？

四、实训题

1．创建本地账户 user1、user2 和 user3。

2．设置密码策略（如启用密码复杂性要求、最短密码长度为 10 等）。

3．更改本地账户 user1、user2 和 user3 的密码。

4．创建 ceshi 组。

5．将本地账户 user1 和 user3 分别归到 Administrators 和 ceshi 组。

6．NTFS 权限的设置

请自行创建一个目录，分数次进行不同的 NTFS 权限设置，并在每次设置完毕后，分别从服务器和工作站上观察与测试在该目录下分别能进行什么样的文件操作，并将结果记录于表 2.7 中。

表 2.7　NTFS 权限设置

指定的共享权限	在服务器端所能进行的操作	在工作站端所能进行的操作

7．创建隐藏共享文件夹

在本部分实验中，要求创建一个名为“secret”的共享文件夹并隐藏共享名，相应的操作步骤可参考如下。

（1）隐藏共享文件夹的创建

① 打开 Windows Server 2003 资源管理器，选择驱动器 E；

② 在“文件”菜单中，选择“新建文件夹”，创建一个新的文件夹；

③ 输入“secret”为目录名，按 Enter 键；

④ 选中“secret”文件夹，单击鼠标右键，选择共享；

⑤ 选择“共享为”；

⑥ 在共享名中，输入“secret $”（$表示对网络用户隐藏共享名）；

⑦ 在描述中输入系统实用程序，单击“确定”按钮。

（2）测试具有隐藏共享名的文件夹的可视性

① 单击开始菜单，选择“运行”命令项；

② 在打开文本框中，输入网络路径“\\studentx”，单击“确定”按钮；

③ 观察“secret $”有没有出现；

④ 退出所有应用程序；

⑤ 与隐藏的共享文件夹建立连接；

⑥ 单击“开始”菜单，选择“运行”命令项；

⑦ 在打开的文本框中，输入“\\studentx\secret$”，单击“确定”按钮；

⑧ 观察此时能否访问 secret $共享文件夹；

⑨ 退出 Windows NT/2000 资源管理器，并注销用户。

8．共享权限与 NTFS 权限的联合操作

利用共享权限与 NTFS 权限进行文件系统的访问管理。

（1）文件系统的创建

在 NTFS 格式的磁盘上创建以下目录结构，并复制一些文件到这些目录下：Foldba、Foldbb、Foldbc、Foldbd、Foldbe。

（2）完成文件系统的访问管理

请综合利用前面所学的创建共享权限和目录与文件属性的方法，对上述文件系统中的目录与文件进行必要的设置，使得：

① 从 Windows NT 或 Windows 98 或非 Windows NT 平台都可以看到共享文件名；

② Administrators 对所有文件、目录具有完全控制权限；

③ 所有 User 组的用户都可以运行 Foldbc 目录中的程序，但不能修改 Foldbc 目录中的文件；

④ 只有 Accounting managers 组的成员能访问 Foldbd 和 Foldbe 目录，但不能修改这些目录中的文件；

⑤ 所有 User 组的用户在 Foldaa 目录中都可以创建和修改他们自己的文件，但不能修改其他用户的文件；

⑥ 所有 User 组的用户不能修改 Foldaa\ Foldba 目录中的文件；

⑦ 只有用户 UserA 能修改 Foldaa\ Foldbb 目录下的文件。

注：Folda 目录等级如图 2.41 所示。

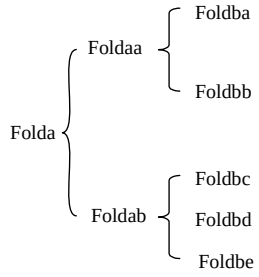

图 2.41　Folda 目录等级

项目 3　网络打印的配置与管理

3.1　项目内容

1．项目目的

在了解逻辑打印机、打印驱动程序和打印服务器的概念的基础上，掌握本地打印机的添加和网络打印机的添加过程；掌握网络打印机的配置与管理。

2．项目任务

某公司组建了单位内部的办公网络，但办公设备（尤其是打印设备）不能每人配备一台，需要在同一办公室内配置网络打印供办公室的人员使用。

3．任务目标

① 了解打印驱动程序和打印服务器的概念；
② 掌握本地打印机的添加过程；
③ 掌握在 Windows Server 2003 系统下配置网络打印服务的方法。

3.2　相关知识

3.2.1　打印系统的基本概念

打印系统是网络管理的重要组成部分，在介绍网络打印的配置之前，先了解打印系统的相关基本概念。

1．打印设备

打印设备指的是产生打印文档的硬件设备。

Windows Server 2003 支持以下打印设备：

① 本地打印设备，指的是连接在打印服务器物理端口的打印设备；
② 网络打印设备，指的是通过网络而不是通过物理端口连接到打印服务器的打印设备。

网络打印设备要求有它们自己的网络适配器和网络地址，或者需要将它们连接在某个外部的网络适配器上。

2．打印机

打印机指的是操作系统和打印设备之间的软件接口。打印机定义文档何时到达打印设备，以及通过什么方式到达打印设备。

3．打印服务器

打印服务器指的是特定的计算机，打印机和客户机驱动程序就在该计算机上。打印服务器接收和处理来自客户计算机的文档。需要在打印服务器上建立和共享与本地打印设备和网络接口打印设备相关联的网络打印机。

4．打印机驱动程序

打印机驱动程序指的是一个或多个文件。Windows Server 2003 要利用这些文件中的信息，将打印命令转换为特定的打印机语言。通过这种转换，才使得打印设备能够打印文档。打印机驱动程序是针对各个具体型号的打印设备的。在打印服务器上必须要有相应的设备。

3.2.2 网络打印共享方案

Windows Server 2003 系统为用户提供了强大的打印管理功能，用户可以在网络上共享打印资源。网络打印要求有专门的服务器来管理打印机，网络中的其他计算机作为客户机使用网络打印服务。

要实现一台打印设备供给多台计算机使用，现在主要有两种解决方案。

（1）打印设备直接连接在一台计算机上，通过在计算机上设置打印机共享，可以实现网络打印，如图 3.1 所示。由于作为打印服务器的计算机一般还要进行其他工作，因此占用资源较多，打印效率较低。

（2）打印机通过专业的打印服务器直接连接到网络上，打印机不再是计算机的外部设备，而是网络中的独立成员，用户可以通过网络直接访问该打印机，打印效率更高，更适合企业级局域网应用，如图 3.2 所示。打印服务器又分为外置打印服务器和内置打印服务器两种。

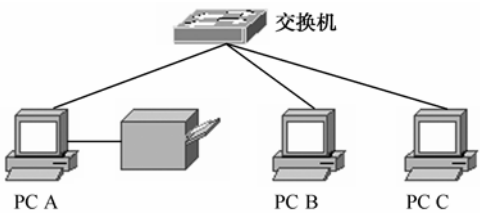

图 3.1 网络拓扑图（1）

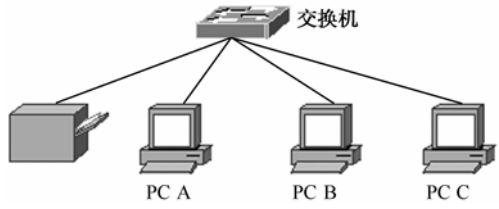

图 3.2 网络拓扑图（2）

3.2.3 配置网络打印机的基本要求

在 Windows Server 2003 网络中设置打印机时，有一定的硬件要求。

（1）至少有一台计算机作为打印服务器。如果打印服务器要管理大量的作业，则推荐使用专用的打印服务器。Windows Server 2003 作为打印服务器系统可处理大量的连接，并且只运行 Windows、UNIX、NetWare 客户转向器以及打印服务的计算机。如果使用 Windows XP Professional 作为打印服务器系统，则仅限于支持来自其他计算机的有关文件和打印服务的 10 个并发连接，它不支持 Mac、NetWare 客户，但支持 Windows、UNIX 计算机。

（2）足够的 RAM。如果打印服务器管理大量的打印机或者许多大的文档，则服务器需要的 RAM 可能比 Windows Server 2003 为处理其他任务所要求的 RAM 更多。

（3）足够的硬盘空间。打印服务器上应有足够的磁盘空间，以保证 Windows Server 2003 能够存储发送给打印服务器的文档，直到打印服务器将数据发送给打印设备。

3.2.4 配置网络打印机准则

作为计算机网络管理员，在配置网络打印机时应掌握以下准则。

1．选择打印机名称

Windows XP 和 Windows Server 2003 支持使用长打印机名称，这允许用户创建包括空格

和特殊字符的打印机名。但是如果在网络上共享打印机，某些客户端将无法识别或不能处理长文件名称，并且用户可能遇到打印问题。而且某些程序不能打印到名称超过 32 个字符的打印机。

（1）如果在网络上有许多客户端共享打印机，应使用 32 个或更少的字符作为打印机名称，而且在名称中不能包括空格和特殊字符。

（2）如果与 MS-DOS 计算机共享打印机，则不要用超过 8 个字符的打印机共享名。

（3）如果打印机名称长度超过一定的字符数，一些 Windows 3.X 版本的程序将无法打印到打印机。

2．确定放置打印机的位置

需要将打印机放置在将要使用它们的用户附近。但是，还需确定打印机相对于网络中的打印服务器和用户计算机的位置，同时要使其对网络环境中的打印影响降到最低。

检查网络的基础结构，尽量使打印作业跳过多个互联网络设备。如果有一组需要较高打印量的用户，可以让他们只使用其所在网段中的打印机来将其隔离，使其对别的用户的影响降到最低。

3．为打印机位置确定命名约定

需要进行打印机位置跟踪，并使用下列规则来设置打印机的命名约定。

（1）位置名称的格式为：name/name/…（必须使用斜杠“/”作为分隔符）。

（2）名称可以由除斜杠/之外的任意字符组成，名称的等级数限制为 256。

（3）name 的最大长度是 32 个字符，整个位置名称的最大长度是 260 个字符。

（4）因为位置名称由最终用户使用，所以位置名称应当简单且容易识别。避免使用只有设备管理人员知道的特殊名称。

3.3　方案设计及准备

1．设计

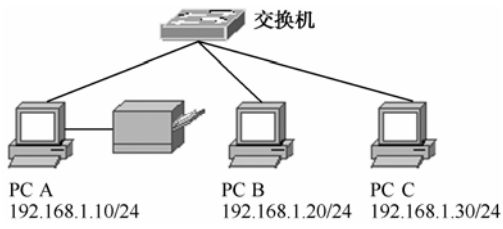

图 3.3　网络拓扑图

为了模拟本项目的任务，假定用 3 台计算机组成一个局域网，但只有一台联想 LJ2210 打印机，现在需要把这台打印机安装到一台计算机 PC A 上，共享到局域网上，并设置打印机的使用时间为上班时间。

根据以上要求，本项目实施的网络拓扑图如图 3.3 所示。3 台计算机的 IP 地址如图 3.3 所示。

2．设备清单

为了搭建如图 3.3 所示的网络拓扑图，需要如下设备：

① PC 计算机 3 台，其中 PC A 安装 Windows Server 2003 操作系统，其余两台为 Windows XP 操作系统；

② 交换机 1 台；

③ 双绞线直通线 3 条；

④ 打印机 1 台。

3.4 项目实施

步骤 1：硬件安装

按照图 3.3 所示用 3 条直通线将 3 台计算机连接到交换机上，检查网卡和交换机的指示灯连接状态，判断网络是否连通。

步骤 2：TCP/IP配置

（1）配置 PC A 的 IP 地址为 192.168.1.10，子网掩码为 255.255.255.0；配置 PC B 的 IP 地址为 192.168.1.20，子网掩码为 255.255.255.0；配置 PC C 的 IP 地址为 192.168.1.30，子网掩码为 255.255.255.0。

（2）PC A、PC B 和 PC C 之间互相 ping，检查网络的连通性。

步骤 3：通过“网上邻居”访问局域网计算机

双击桌面上的“网上邻居”图标，检查能否看到每台计算机名。

步骤 4：安装共享服务与客户端

（1）安装“Microsoft 网络的文件和打印及共享”服务。右击联网图标，选择“状态”选项或双击联网图标，打开“本地连接状态”窗口，单击“属性”按钮，打开“本地连接属性”窗口。单击“添加”按钮，打开“选择网络组件类型”对话框，如图 3.4 所示。在“单击要安装的网络组件类型”框中，选中“服务”选项，单击“添加”按钮，打开“选择网络服务”对话框，如图 3.5 所示。选中“Microsoft 网络的文件和打印及共享”，单击“确定”按钮。

（2）安装“Microsoft 网络客户端”。单击“添加”按钮，打开“选择网络组件类型”窗口，在“单击要安装的网络组件类型”框中，选中“客户端”选项，单击“添加”按钮，打开“选择网络客户端”窗口，选中“Microsoft 网络客户端”选项，单击“确定”按钮。

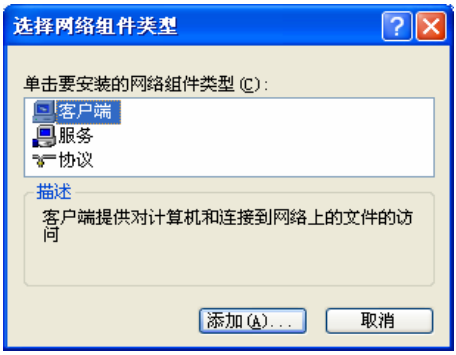

图 3.4 “选择网络组件类型”对话框

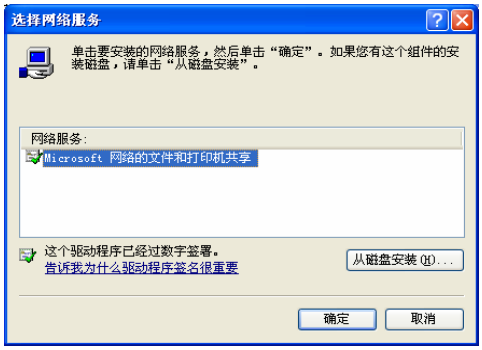

图 3.5 “选择网络服务”对话框

步骤 5：在PCA计算机上安装本地接口打印机

（1）选择“开始→设置→打印机和传真”命令，打开“打印机和传真”对话框，单击“添加打印机”，打开“添加打印机向导”对话框，单击“下一步”按钮，打开“本地或网络打印机”对话框，选中“连接到此计算机的本地打印机”单选按钮，并选中“自动检测并安装即

插即用打印机”选项，如图 3.6 所示。

（2）单击“下一步”按钮，计算机进行自动检测，如果检测到打印机会自动安装完成，未检测到可以手动安装，则单击“下一步”按钮，打开“选择打印机端口”对话框，选择打印机连接的端口，如 LPT1，如图 3.7 所示。

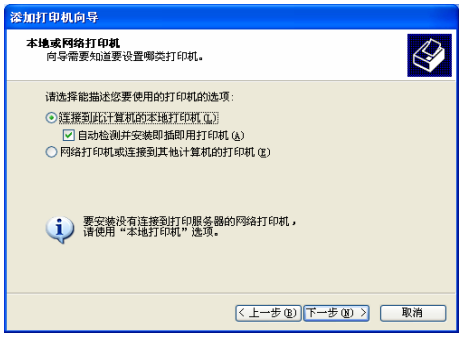

图 3.6　“本地或网络打印机”对话框

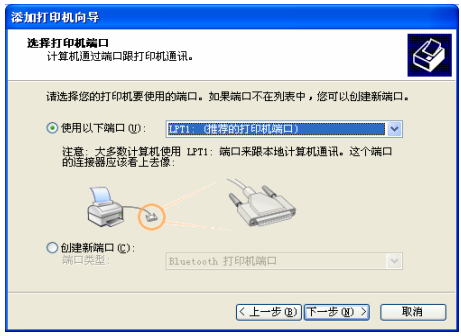

图 3.7　“选择打印机端口”对话框

如果是 USB 接口的打印设备，可以直接连接到计算机上，打开电源后，系统将自动进行安装。

（3）单击“下一步”按钮，打开“安装打印机软件”对话框，在“厂商”列表中选择“联想”，在“打印机”列表框中选择“Legend LJ2210P”，如图 3.8 所示。

（4）单击“下一步”按钮，打开“命名打印机”对话框，在“打印机名”文本框中输入打印机的名称，也可采用默认名称，如 Legend LJ2210P，如图 3.9 所示。选择“是”单选按钮将该打印机设置为默认打印机或选择“否”单选按钮将该打印机设置为非默认打印机。

（5）单击“下一步”按钮，打开“打印测试页”对话框，选择“是”或“否”打印测试页。

（6）单击“下一步”按钮，弹出下一页，单击“完成”按钮，计算机会复制驱动程序，完成安装。

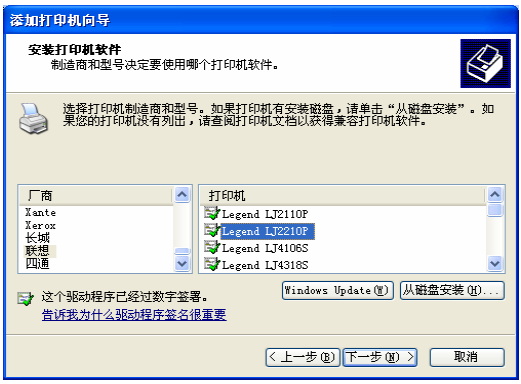

图 3.8　“安装打印机软件”对话框

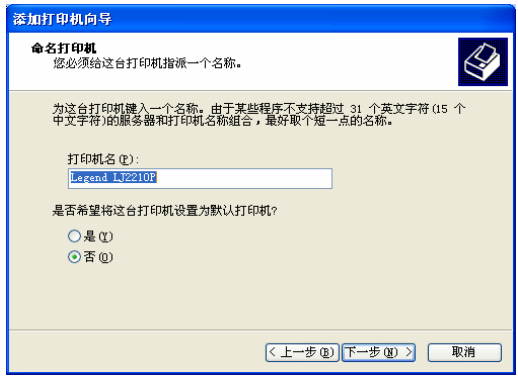

图 3.9　“命名打印机”对话框

（7）如果打印机型号不在系统列表中，单击“从磁盘安装”按钮，打开“从磁盘安装”对话框，单击“浏览”按钮选择厂商的驱动盘的位置，一般为光驱，如图 3.10 所示。单击“确定”按钮安装驱动程序。安装完成后打印机会添加到“打印机和传真”窗口中。

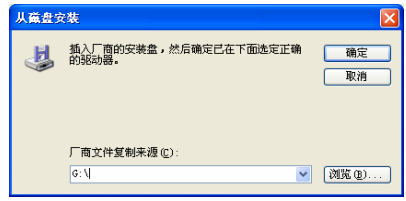

图 3.10　“从磁盘安装”对话框

步骤 6：PCA共享本地打印机

（1）选择“开始→设置→打印机和传真”命令，打开“打印机和传真”窗口，右击“Legend LJ2210P”选项，在弹出的快捷菜单中选择“共享”选项，打开“Legend LJ2210P 属性”对话框，如图 3.11 所示。

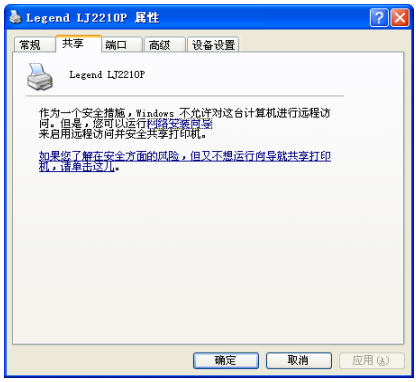

图 3.11　“Legend LJ2210P 属性”对话框

（2）作为安全措施，Windows 不允许对这台计算机进行远程访问，但是，可以运行“网络安装向导”来启用远程访问并安全共享打印机，双击“网络安装向导”链接，打开“网络安装向导”对话框，按照提示一步一步进行，单击“下一步”按钮，打开“选择连接方法”对话框，选择计算机连接到 Internet 的方法。

（3）连续单击“下一步”按钮，直到打开“文件和打印机共享”对话框，如图 3.12 所示，选中“启用文件和打印机共享”单选按钮，单击“下一步”按钮，单击“完成”按钮，系统进行配置。

（4）打开“Legend LJ2210P 属性”对话框，选择“共享”选项卡，如图 3.13 所示。选中“共享这台打印机”单选按钮，在“共享名”文本框中输入共享的打印机名，也可选用默认名称。

（5）设置完成后，在此打印机的图标下会显示共享标记。

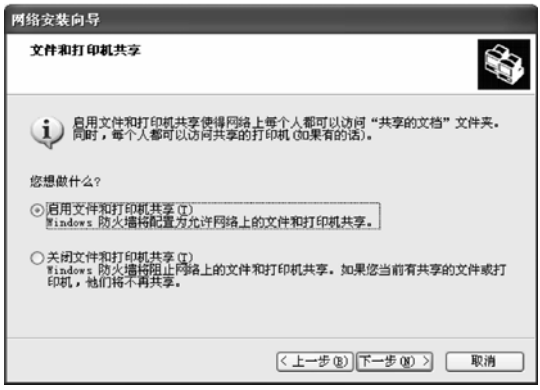

图 3.12　“文件和打印机共享”对话框

图 3.13　“共享”选项卡

步骤 7：PC B、PC C安装网络打印机

在计算机 PC B 和 PC C 上添加网络打印机的步骤相同，下面以在 PC B 上添加打印机为例。

（1）选择“开始→设置→打印机和传真”命令，打开“打印机和传真”窗口，单击“添加打印机”，打开“添加打印机向导”对话框，单击“下一步”按钮，打开“本地或网络打印机”对话框，选中“网络打印机或连接到其他计算机的打印机”单选按钮。

（2）单击“下一步”按钮，打开“指定打印机”对话框，如图 3.14 所示。

（3）选中“浏览打印机”单选按钮，单击“下一步”按钮，打开“浏览打印机”对话框，在“共享打印机”列表框中选择需要连接的打印机，如图 3.15 所示。单击“下一步”按钮，然后单击“完成”按钮即可。

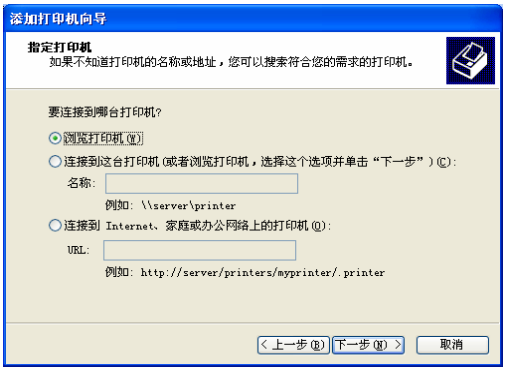

图 3.14　“指定打印机”对话框

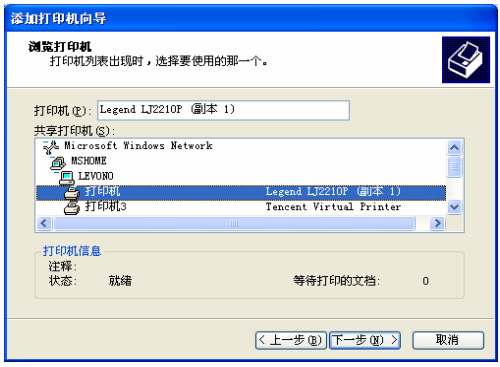

图 3.15　“浏览打印机”对话框

（4）可在图 3.14 中选中“连接到 Internet、家庭或办公网络上的打印机”单选按钮，在“名称”框中直接输入网络上可共享的打印机，如\\192.168.1.10\ Legend LJ。

（5）单击“下一步”按钮，会在“打印机和传真”窗口添加网络上的打印机。

注意

① 如果客户端的计算机安装的操作系统是 Windows Server 2003 和 Windows XP，这两种系统有自动搜索网络共享打印机的功能，能够自动连接到共享打印机、自动安装打印驱动程序。

② 如果客户端的计算机安装的操作系统是 Windows 2000，则需要手动连接共享打印机，在连接共享打印机的过程中，客户端的计算机会自动从所连接的打印服务器上下载驱动程序。

步骤 8：设置打印机的优先级

公司员工共用一台打印机，在同一时刻有多人要使用打印机，有的用户有紧急的文件需要打印，其打印作业却不得不排队等侯，这时管理员可以采用设置打印机优先级的方式，可以让有紧急打印作业的用户抢占打印机，先打印文档，让其他用户等待。

设置打印机优先级的方法是：在服务器上为一台打印设备同时安装多个逻辑打印机程序，并设置不同的打印机名和共享名，然后设置不同的优先级。需要紧急打印的用户连接优先级高的逻辑打印机，其他用户连接优先级低的逻辑打印机。

（1）使用“添加打印机向导”，为打印设备同时添加多个打印机程序。

（2）打开各个打印机的属性对话框，选择“高级”选项卡，分别设置一个“优先级”，其值从 1 到 99，数值越大，优先级越高，如图 3.16 所示。

步骤 9：设置打印时间

如果要求打印机只能在上班时间内使用，其他时间限制使用，管理员可以通过设置打印机的打印时间来实现。

（1）打开打印机的属性对话框，选择“高级”选项卡，如图 3.17 所示。

（2）如图 3.17 所示，设置使用时间为从 8：00～17：00。

图 3.16　设置优先级

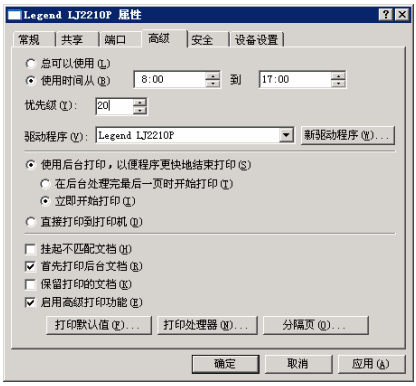

图 3.17　设置打印时间

打印机在工作时间比较忙碌，如果有的用户要打印的文档较大，或者文档不是急件，希望文档送到打印服务器后不立即打印，而是在打印机不忙的时候再打印，可以通过设置打印时间来解决。设置打印时间的原理是在一台打印服务器上安装多个相同的打印驱动程序，并给它们取不同的打印机名和共享名，从而建立多个逻辑打印机，将要求打印时间不同的文档送到不同的打印机上。

步骤 10：设置打印权限

在步骤 8 中已经为不同的逻辑打印机设置了不同的打印机，但在实际操作中，几乎每个用户都喜欢连接优先级高的逻辑打印机。这时可以对不同用户设置不同的共享打印机使用权限，限制优先级高的打印机只有特定用户才能连接打印。

（1）在“打印机和传真”窗口中，右击优先级高的打印机，选择“属性”，打开“属性”对话框。

（2）选择“安全”选项卡，如图 3.18 所示，可以看到默认的是每个用户都有“打印”的权限。

在这里可以设置三种权限：

- 打印。可以连接打印机和打印文档；管理用户自己的打印文档。
- 管理打印机。可以连接打印机和打印文档；管理所有的打印文档；更改打印顺序、打印时间等设置；设置打印机的共享；更改打印机属性；删除打印机；更改打印机的安全权限。

图 3.18　打印权限设置

➢ 管理文档。可以管理所有的打印文档；更改所有文档的打印顺序、打印时间等设置。

（3）在图 3.18 中，删除 everyone 组的打印权限，然后“添加”指定的用户或组到列表中，给予“打印”权限。

这时，就只有拥有权限的用户才能连接该打印机，并且使用这个优先级高的打印机来提交打印文档。

步骤 11：管理打印作业

打印机在打印过程中，有时需要对打印作业进行各种管理，例如，用户提交了错误的打印作业，必须将它取消；或者在同一打印机的打印队列中，管理员需要调整文档的打印次序等。

Windows Server 2003 通过打印机管理器对打印机上的打印作业进行管理。具有打印机的“管理打印机”或“管理文档”权限的用户，可以管理打印机上的打印作业。

（1）在“打印机和传真”窗口，双击打印机图标，打开“打印机管理器“窗口，在窗口中会列出当前的打印文档队列。

（2）管理单个打印文档。如果某份文档在打印时出了问题，可以暂停打印，等解决问题后再重新打印，或者取消打印。在“打印机管理器”窗口中，选择要处理的文件，单击鼠标右键，如图 3.19 所示。或选中某个文档后，打开“文档”菜单，如图 3.20 所示。

图 3.19　单个打印文档操作 1

图 3.20　单个打印文档操作 2

➢ 暂停：暂停打印该文档。

➢ 继续：继续打印被暂停的文档。

➢ 重新启动：从第一页开始打印。

➢ 取消：取消打印该份文档，文档的状态显示为“正在删除”。

（3）管理所有打印文档。如果打印设备出了问题，则可以暂停打印所有的文档，待问题解决后再重新打印，或者取消打印。在“打印机管理器”窗口中，打开“打印机”菜单，如图 3.21 所示。

图 3.21　所有打印文档操作

➢ 暂停打印：选用后会暂停打印所有的该文档。

➢ 取消所有文档：取消打印所有在该打印机排队等待打印的文档，这些文档都会被删除。

步骤 12：设置打印作业的属性

打印机安装完成后，还可以根据用户或公司的需求进一步设置打印机，这些设置都在打印

机的“属性”对话框里操作。右击相应的打印机，选择“属性”，打开“打印机属性”对话框。

（1）选择“常规”选项卡，如图 3.22 所示，可以设置打印机的名称、位置信息和注释信息。单击“打印首选项”按钮可以设置打印机使用的纸张类型；单击“打印测试页”按钮可以测试打印是否正确。

（2）选择“共享”选项卡，如图 3.23 所示，可以设置打印机是否共享。一旦停止共享，网络上的其他用户将无法访问此台打印机。单击“其他驱动程序”按钮，可以添加其他操作系统使用的打印机驱动程序。

图 3.22　打印机属性—常规

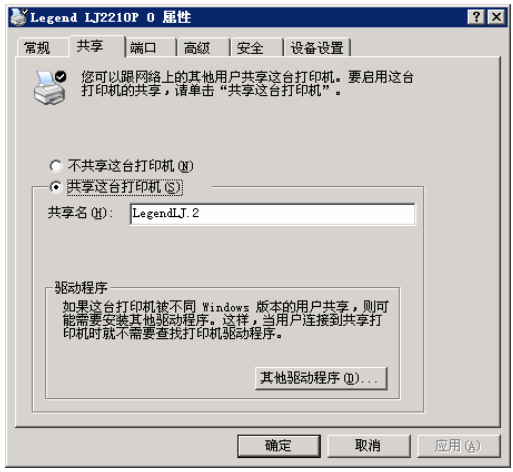

图 3.23　打印机属性—共享

（3）选择“端口”选项卡，如图 3.24 所示，普通打印机都是通过 LPT1 端口和计算机相连，虽然计算机的主板上只有一个 LPT1 端口，但是可以通过扩展卡扩展出 LPT2 和 LTP3 接口，这样就可以同时连接多台打印机。

（4）选择“高级”选项卡，如图 3.25 所示，可以设置打印机的工作时间和优先级。

- 时间可以设置每天的某个时间段打印机可以工作，不过只能设置一个时间段。
- 一般情况下打印的顺序是按照时间的顺序，即先来先打。但有时个别用户需要打印一些比较紧急的文件，这时就可以通过设置打印机的优先级来实现。设置方式是：创建两（多）个（逻辑）打印机，这两个（逻辑）打印机同时映射到同一台物理打印设备，并设置不同的优先级，用这种方式可以让同一台打印设备处理多个（逻辑）打印机所送来的文档，即可以处理多个不同优先级的打印任务。
- 使用后台打印，以便程序更快地结束打印。后台打印的作用是先将收到的打印文档存储在硬盘内，然后将其送到打印设备打印。文档送往打印设备的工作由后台处理程序负责，并且在后台运行。
- 直接打印到打印机。表示文档是直接送到打印设备的，而不会先送到后台打印区内。
- 挂起不匹配文档。选择该复选框后，如果所有打印文档的文件格式的设置与打印机不符合，则该文档会被搁置不打印。例如，将打印机设置为使用信纸尺寸的纸张，但是文件格式却不是设置成信纸尺寸的纸张，则打印机收到该文档后，并不会将其送往打印设备。
- 首先打印后台文档。先打印已经完整送到后台的文档，而数据尚未完整收齐的文档稍后再打印，即使这份不完整的文档的优先级较高或者先收到也是如此。如果撤销该复选框，则打印的先后顺序取决于其优先级与送到打印机的顺序。

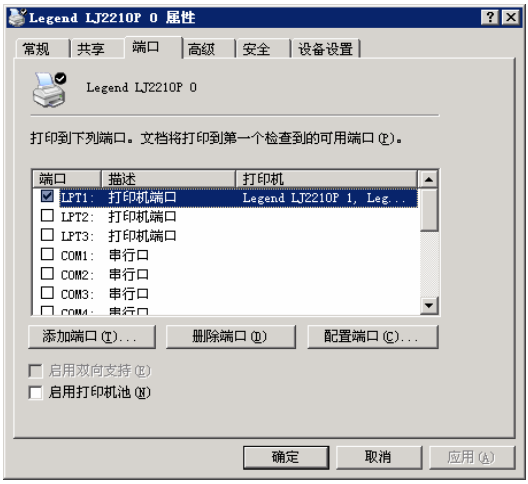

图 3.24　打印机属性—端口

图 3.25　打印机属性—高级

- 保留打印的文档。当打印文档被送往打印服务器时，它会先被暂时存储到服务器的硬盘内排队等待打印，这个操作就是后台处理（临时文件称为后台文档），轮到时再将其送到打印设备打印。该选项可以让用户决定是否在文档送到打印设备后，就将后台文档从硬盘中删除。
- 启用高级打印功能。当启用高级的打印功能后，文件会采用增强性图元文件（Enhanced Metafile，EMF）的格式转换打印的文件，并且支持一些其他的高级打印功能。

（5）选择“安全”选项卡，可以指派打印机的使用权限。在“安全”选项卡里，就可以看到打印机的权限列表，前面已经介绍过。

步骤 13：设置文档打印默认值

文档打印默认值描述了如何使用打印机的硬件执行打印任务。典型的文档默认属性包括页面方向、页序、单面或双面打印、纸张来源、纸张规格、打印份数、设置默认的打印首选项等。

（1）在“打印机和传真”窗口，右击打印机图标，选择“打印机首选项”选项，打开打印机首选项对话框，如图 3.26 所示。

（2）单击“高级”按钮，打开打印机高级选项对话框，如图 3.27 所示。

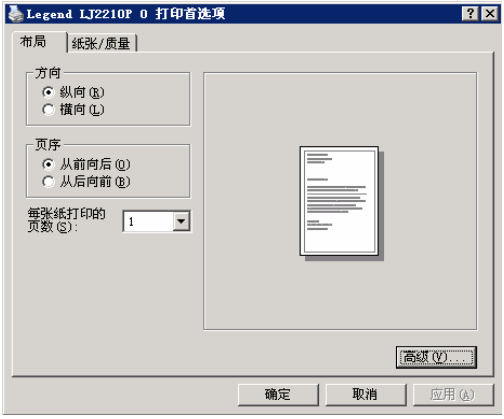

图 3.26　打印机首选项对话框

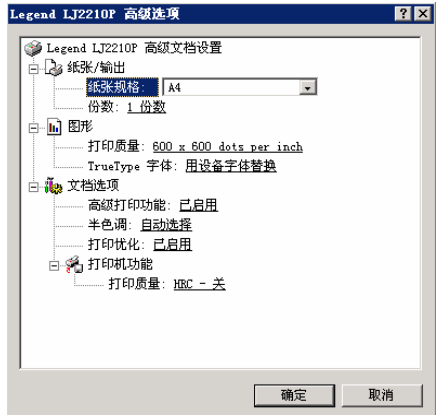

图 3.27　打印机高级选项对话框

3.5 扩展知识及任务训练

3.5.1 训练 1：安装有网络接口卡的打印机

在一些大型网络中，对打印机的打印速度要求很高。而一般使用并口打印电缆与电脑连接的打印机的速度较慢，所以在大型网络里，一般采用有网络接口的打印机。

这种网络打印机具有专用的网络接口卡（一种与网卡十分类似的接口卡），可以通过网线直接接入网络。由于网线的传输速度远远大于并口打印电缆的传输速度，所以这种打印机打印速度也非常快。此类打印机被称为“网络接口打印机”。

网络接口打印机大部分都支持 TCP/IP 通信协议，它相对于每一台客户机都是本地打印机，因为它不需要上面提到的介于客户机的打印服务器。每一台客户机都和打印机直接联系，这也避免了由于打印服务器的故障而导致打印服务中断的可能。

客户端安装具有网络接口卡的打印机的步骤如下。

步骤 1：选择“开始→设置→打印机和传真”命令，打开“打印机和传真”窗口。

步骤 2：在“打印机和传真”窗口中，单击“添加打印机”，打开“添加打印机向导”对话框。

步骤 3：单击“下一步”按钮，打开“本地或网络打印机”对话框，选中“连接到此计算机的本地打印机”单选按钮，并取消下面的“自动监测并安装我的即插即用打印机”选项。打印机虽然通过网络接口连接，但还是由本服务器来管理。

步骤 4：单击“下一步”按钮，打开“选择打印机端口”对话框，如图 3.28 所示，选择打印机的端口类型，这里选择“创建新端口”，并在右侧的下拉列表中选择 Standard TCP/IP Port。

步骤 5：单击“下一步”按钮，打开“添加标准 TCP/IP 打印机端口向导”对话框，如图 3.29 所示。

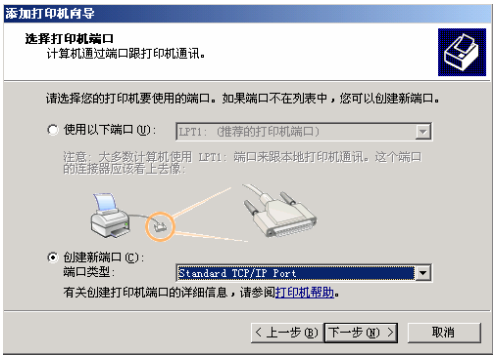

图 3.28 “选择打印机端口”对话框

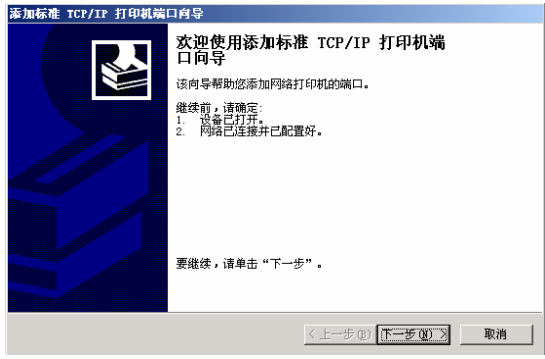

图 3.29 “添加标准 TCP/IP 打印机端口向导”对话框

步骤 6：单击“下一步”按钮，打开“添加端口”对话框，如图 3.30 所示，输入网络接口打印机的名称或 IP 地址，并设置端口名。

步骤 7：单击“下一步”按钮，打开“需要额外端口信息”对话框，如图 3.31 所示，在“设备类型”中选择“标准”，在“标准”右侧下拉列表中选择打印机使用的网络接口卡的厂商和型号，完成后单击“下一步”按钮。接下来的步骤与添加一般的打印机类似，如安装打印机驱动程序，将其设为共享打印机等。

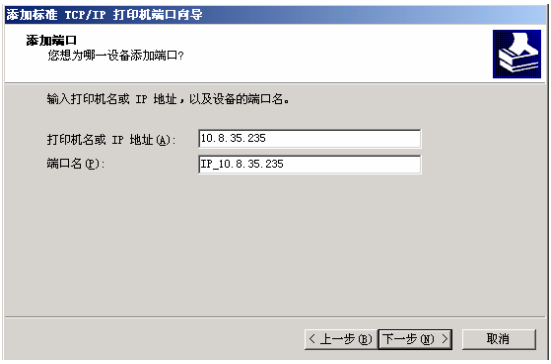

图 3.30 “添加端口”对话框

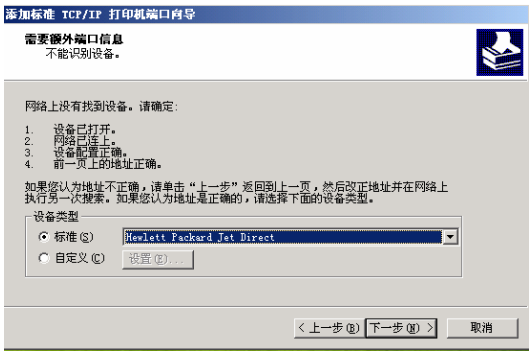

图 3.31 “需要额外端口信息”对话框

注意 新购置的具有网络接口卡的打印机，需要设置好相应的 IP 地址。可以使用打印机附带的软件，先设置可以和当前网络通信的 IP 地址，然后再到其他客户机上安装打印机。

3.5.2 训练 2：设置打印机池

某公司的打印任务繁重，购买了 3 台同型号的打印设备，由一台服务器管理，为员工提供打印服务。如果为 3 台打印机分别建立一台共享打印机，由用户随意连接其中一个进行打印，则可能会造成打印任务负载不均衡的问题。在这种情况下，管理员决定使用打印机池的方式，即用一台共享打印机来同时管理 3 台设备，所有用户连接到一台共享打印机上，由这台打印机来平均分配打印任务，如图 3.32 所示。

打印机池是指一台打印机对应多台打印设备。这里的打印机是指控制面板中的逻辑打印机，打印设备是指真正的物理打印机。打印机池主要用于当一台打印机的速度不能满足打印服务的要求时，可以用两台或者多台打印设备来提供服务。

注意 打印机池的功能是将多台打印机模拟成一台打印机工作，这里的打印机必须为相同厂商和相同型号的打印机。端口可以是本地端口，也可以是远程端口。

（1）将 3 台设备都连接到计算机上。

（2）利用“添加打印机向导”为其中一台设备安装打印机驱动程序。

（3）在“打印机和传真”窗口，右击已安装好的打印机，选择“属性”，打开“打印机属性”对话框，选择“端口”选项卡，如图 3.33 所示。

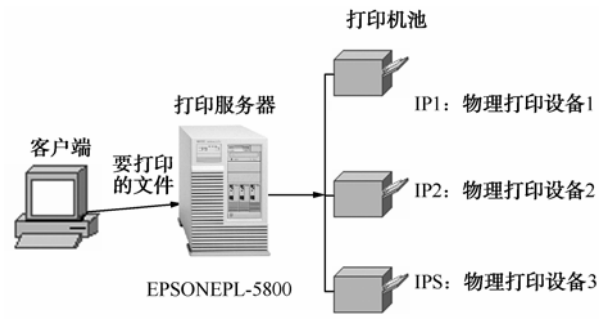

图 3.32 打印机池示意图

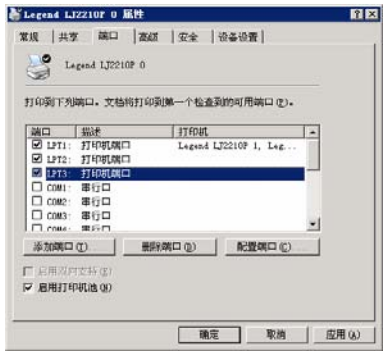

图 3.33 打印机属性—端口

（4）选中“启用打印机池”复选框，再选中打印设备所连接的端口，单击“确定”按钮。

3.5.3 通过Web浏览器管理打印机

客户端可以远程管理打印机，也可以将作业发送到远程的打印机上进行打印。通过 Web 浏览器管理打印机，用户可以利用下列两种方法：

（1）http://服务器的名称（IP 地址）/打印机的共享名，例如，http://10.8.35.25/ HPColorL。输入具备管理该打印机权限的用户名称与密码。如果要用域用户账户连接，则在账户名前面加上域名，例如 AAA\administrator，其中的 AAA 是域名。然后就可以通过打开的对话框管理该打印机与正在等待打印的文档。

（2）http://打印服务器的名称（IP 地址）/printers，例如，http://10.8.35.25/printers/。在输入用户名称与密码后，屏幕上会显示打印服务器内所有的共享打印机，可以选择一台有权管理的打印机来执行管理的工作。

习　题

一、填空题

1．规划打印服务器安装策略需要考虑_____、_____和_____。

2．网络打印机安装的两种形式为_____和_____。

二、选择题

1．关于打印机的说法，下面的描述正确的是（　　）。

A．打印机就是我们所购买的打印设备

B．打印机是介于操作系统与打印设备之间的软件接口

C．计算机第一次连接打印服务器上的共享打印机时，不会在本地计算机上安装打印驱动程序

D．使用网络接口的打印设备时，不需要通过打印服务器

2．下面哪一个不属于用户对共享打印机的权限？（　　）

A．读取和运行　　B．打印

C．管理打印机　　D．管理文档

3．在默认情况下，具有管理打印机权限的成员组包括（　　）。

A．Everyone 组　　B．Administrator 组

C．Print Operator 组　　D．CreatoeOwner 组

4．某公司的打印量非常大，决定使用“打印机池”的方法来分担打印任务、提高打印效率。则该公司在购买打印设备时，有什么要求？（　　）

A．只允许购买同一厂商、同一型号的打印设备。

B．最多只能购买 3 台打印设备。

C．允许购买使用同一打印驱动程序的任意打印设备。

D．打印设备的型号和数量可以任意选择。

5．一家公司到每月月末，财务部都要长时间占用机器，打印大量的财务报表。而网络管理员也要在工作时间打印本月的日志总结，可是由于财务部打印财务报表而不能使用。在这种情况下，管理员如何使自己能够先打印日志总结？（　　）

A．设置“打印时间”，满足打印需要。

B．设置“打印重定向时间”，满足打印需要。

C．设置“打印缓冲池”，满足打印需要。

D．设置“打印优先级”，使管理员的优先级高于财务部门的员工，满足打印需要。

三、思考题

为什么用多个打印机连接同一打印设备？

四、实训题

1．以管理员身份登录打印服务器，设置 user1 没有打印的权限，以 user1 用户登录，打印 D:\data 下的文档。

2．假设你所在的办公室共有 5 个人，每个人都有自己的计算机。现在购买了一台接口类型为并口的打印机，交由你来管理。要求：办公室主任有优先的打印级别，其他人的打印优先级一样；另外，该打印机只有上班时间使用，并且只有你才能管理打印机和打印作业。

按照以上要求，如何设置才能管理好该打印机？

项目 4　磁盘管理

4.1　项目内容

1．项目目的

在了解磁盘管理概念的基础上，掌握主磁盘分区的创建和管理过程；掌握动态磁盘分区的创建和管理；掌握磁盘管理工具的使用。

2．项目任务

某公司组建了单位内部的办公网络，配置了多台服务器，为了更好地发挥服务器的性能，需要对服务器的硬盘进行规划和管理。

3．任务目标

① 了解磁盘管理的基本概念；
② 掌握主磁盘分区的创建与管理；
③ 了解什么是动态磁盘、动态磁盘分区的创建与管理；
④ 掌握如何利用 Windows Server 2003 自带的磁盘管理工具管理磁盘。

4.2　相关知识

数据存储是操作系统的重要功能之一，网络管理员的工作之一就是保证用户和应用程序有足够的磁盘空间保存和使用数据，并且保证数据的安全性和可用性。管理员利用 Windows 操作系统中的磁盘管理工具，可以完成磁盘分区和卷的管理、磁盘配额管理和磁盘的日常维护操作。

磁盘管理是使用计算机的一项日常任务，Windows Server 2003 提供了两种对磁盘的管理方式——基本磁盘和动态磁盘。同时提供了专门的磁盘管理工具，可以进行基本磁盘和动态磁盘的管理、磁盘碎片整理、可移动存储等。

4.2.1　基本磁盘

基本磁盘是 Windows Server 2003 默认的硬盘管理方式，用磁盘分区来分割硬盘。基本磁盘是指包含主磁盘分区、扩展磁盘分区或逻辑分区的物理磁盘。

硬盘在存储数据之前，必须被分成一个或多个分区，叫做磁盘分区。分区（Partition）是在硬盘的自由空间（还没有被分区的空间）上创建的，是将一块物理硬盘划分成多个能够格式化和单独使用的逻辑单元。

基本磁盘中的分区又分为主磁盘分区（基本分区）和扩展磁盘分区两种类型。扩展磁盘分区又可以被划分为若干个逻辑驱动器。主磁盘分区和扩展磁盘分区上的逻辑驱动器又被称为基本卷，在“我的电脑”中用盘符来标示不同的卷。卷的盘符只能是 26 个英文字母中的一

个。由于 A 和 B 已经被软驱占用，因此实际上磁盘可用的盘符是从 C～Z 的 24 个字母。

基本磁盘规定一块硬盘最多可以创建 4 个分区，可以是 4 个主磁盘分区或最多 3 个主磁盘分区加上 1 个扩展磁盘分区。一块硬盘至少要有 1 个主磁盘分区；最多只能有 1 个扩展磁盘分区。Windows 操作系统一般建议安装在主磁盘分区上。在扩展磁盘分区内可以创建多个逻辑分区（逻辑驱动器）。

1．主磁盘分区（主分区）

主磁盘分区是可以用来引导操作系统的分区，一般是操作系统的引导文件所在的分区。通常每块硬盘的第一个分区都设置为主磁盘分区，也就是通常所说的 C 盘。每块基本磁盘可以建立 1～4 个主磁盘分区，每个主磁盘分区都可以引导磁盘上的操作系统，但同时只能有一个主磁盘分区处于激活状态。

多个主磁盘分区的优点是可以互不干扰地安装多套不同的操作系统，用户可以通过激活不同的主磁盘分区而引导不同的操作系统。当某一个分区损害时，不会影响其他主磁盘分区引导操作系统。

2．扩展磁盘分区（扩展分区）和逻辑分区

当主磁盘分区的数量小于 3 个，并且主磁盘分区的容量小于实际物理硬盘的容量时，剩余的物理硬盘空间就可以被划分为扩展磁盘分区。在扩展磁盘分区内部再划分若干个部分，每一部分称为逻辑分区（逻辑驱动器），如“我的电脑”中的 D:、E：等。逻辑分区不能用来直接启动操作系统，但可以将操作系统的引导文件放到主磁盘分区上，而操作系统放到逻辑分区上。

4.2.2 动态磁盘

基本磁盘适用于个人计算机或单硬盘的服务器，功能比较弱。动态磁盘具备更强大的磁盘管理功能。

动态磁盘是从 Windows Server 2000 时代开始具有的新特性，在 Windows Server 2003 中得到了更好的支持。相比基本磁盘，它提供更加灵活的管理和使用特性。可以在动态磁盘上实现数据的容错、高速的读写操作、相对随意的修改卷大小等操作，这些是不能在基本磁盘上实现的。

为了便于区分，微软在动态磁盘上的分区称做卷（Volume）。卷的使用方式与基本磁盘的主磁盘分区或逻辑驱动器相似，分配驱动器盘符，格式化过后才能保存数据。动态磁盘没有卷数量的限制，只要磁盘空间允许，可以在动态磁盘中任意建立卷。

动态磁盘的管理基于动态卷的管理。卷是一个或多个磁盘上的可用空间组成的存储单元，可以格式化为一种文件系统并分配驱动器号。简单的理解可以认为它和基本磁盘的分区类似，但功能更强大、更复杂。动态磁盘上的卷有简单卷、跨区卷、带区卷、镜像卷、RAID-5 卷等类型。

在基本磁盘中，分区是不可跨越磁盘的。然而，通过使用动态磁盘，可以将数块磁盘中的空余磁盘空间扩展到同一个卷中来增大卷的容量。动态磁盘不使用分区表，而是把配置数据记录在 1MB 大小的磁盘管理数据库中。

基本磁盘不可容错，如果没有及时备份而遭遇磁盘失败，会造成极大的损失。但在动态磁盘上可以创建镜像卷，所有内容自动实时被复制到镜像磁盘中，即使遇到磁盘失败也不会

造成数据损失。在动态磁盘上还可以创建带有奇偶校验的带区卷，来保证在提高性能的同时为磁盘添加容错性。

4.3 项目实施

4.3.1 任务 1：初始化新磁盘

1．工作任务

公司的客户购买了一台新电脑，公司要求你负责为客户安装操作系统和软件，完成系统初始化工作。

2．方案设计

一般在安装操作系统时，只划分出 C 区，系统安装完成后，在“磁盘管理”工具中继续划分剩余的磁盘空间。

一般建议将磁盘分为一个主分区和一个扩展分区，再将扩展分区分为至少 3 个逻辑驱动器。这样至少分出 C、D、E、F 4 个逻辑盘，其中 C 盘安装操作系统和系统软件；D 盘安装各种应用软件；E 盘存储用户的数据；F 盘作为系统备份；建议分区大小在 10GB～50GB 之间。

3．实施过程

步骤 1：启动“磁盘管理”管理工具

（1）选择“开始→程序→管理工具→计算机管理”命令，或者右击“我的电脑”，在弹出的快捷菜单中选择“管理”，打开“计算机管理”控制台窗口，如图 4.1 所示。

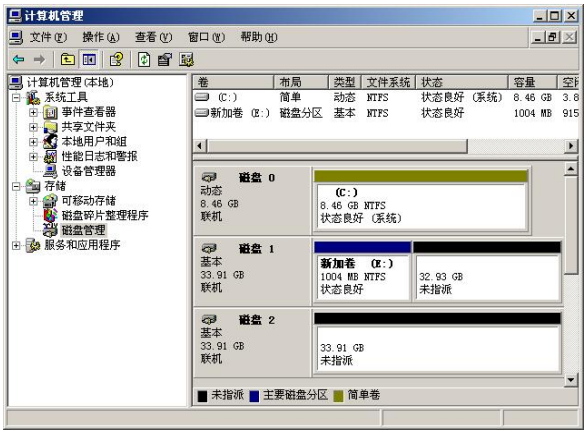

图 4.1　磁盘管理控制台

（2）展开“存储”选项，单击“磁盘管理”选项，窗口右部有“顶端”、“底端”两个窗格，以不同形式显示磁盘信息。如图 4.1 右侧“底端”窗口中以图形方式显示了当前计算机系统安装了 3 个物理磁盘、各个磁盘的物理大小，以及当前分区的结果与状态。“顶端”以列表的方式显示了磁盘的属性、状态、类型、容量、空闲等详细信息。

（3）在图 4.1 中，打开“查看”菜单中的“顶端”、“底端”子菜单，可选择显示磁盘的方式：磁盘列表、卷列表、图形视图等。如图 4.2 所示。

图 4.2　磁盘管理的设置查看属性

（4）在图 4.1 中，打开“查看”菜单的“设置”选项，打开“设置”对话框，如图 4.3 所示，其中“外观”选项卡页用来设置显示的颜色，“比例”选项卡用来设置显示的比例，如图 4.4 所示。

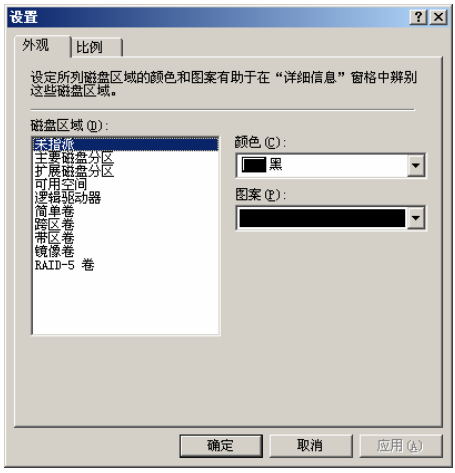

图 4.3　“外观”设置对话框

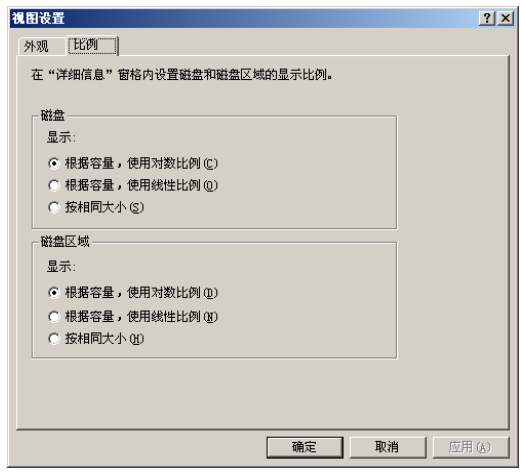

图 4.4　“比例”设置对话框

步骤 2：新建扩展分区

在基本磁盘未使用的空间中，可以创建扩展磁盘分区，但是在一个基本磁盘中只能创建一个扩展磁盘分区。扩展分区创建好后，可以在该分区中创建逻辑磁盘驱动器，并给每一个逻辑磁盘驱动器指派驱动器号。创建扩展磁盘分区的步骤如下：

（1）在磁盘管理控制台中，选取一块未指派的空间，这里选择图 4.5 中磁盘 2 上的未指派空间。右击该空间，在弹出菜单中选择“新建磁盘分区”，打开“新建磁盘分区向导”窗口，如图 4.6 所示，选中“扩展磁盘分区”单选选项。

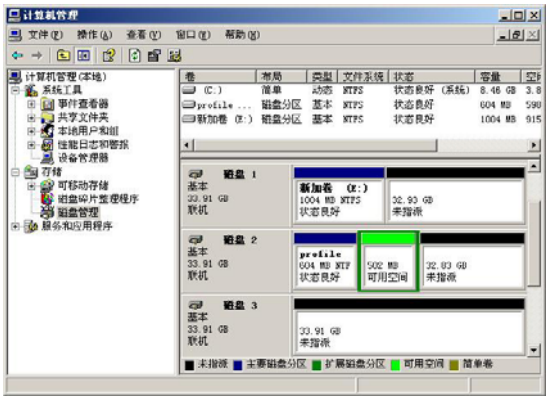

图 4.5　创建扩展分区

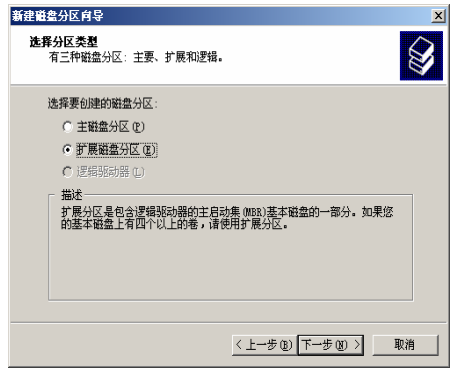

图 4.6　选择分区类型—扩展磁盘分区

（2）单击“下一步”按钮，打开“指定分区大小”对话框，如图 4.7 所示，输入该扩展磁盘分区的容量，其中显示了磁盘分区可以使用的最小值和最大值。可以根据实际情况确定扩展分区的大小。在这里将剩余磁盘空间全部划到扩展分区中。

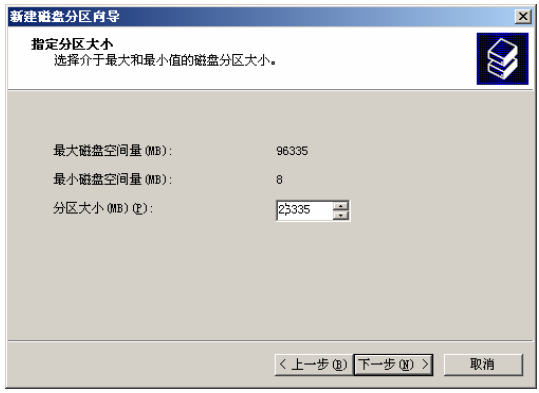

图 4.7　指定分区大小

（3）单击“下一步”按钮，在“正在完成创建磁盘分区向导”对话框中列出上述设置信息，确认无误后，单击“完成”按钮。

步骤 3：更改光盘盘符

在创建逻辑驱动器之前，注意到计算机的光驱此时已经占用了“D:”盘符，而通常习惯于将光驱的盘符放到硬盘的盘符之后，所以，要把光驱的盘符改为“G:”。

（1）在“DVD（D:）”上右击，选择“更改驱动器号和路径”选项。打开“更改 D: 的驱动器号和路径”对话框。

（2）单击“更改”按钮，打开“更改驱动器号和路径”对话框。打开“指派以下驱动器号”的下拉列表框，选择新的驱动器号，如“F:”。

（3）单击“确定”按钮，可以看到光驱的盘符已经被修改了。

步骤 4：在扩展分区上创建逻辑驱动器

这时就可以在刚才创建好的扩展分区上继续创建逻辑驱动器了。

（1）在刚才创建的扩展分区上右击，选择“新建逻辑驱动器”，打开“新建磁盘分区向导”对话框，如图 4.8 所示，选中“逻辑驱动器”单选选项。

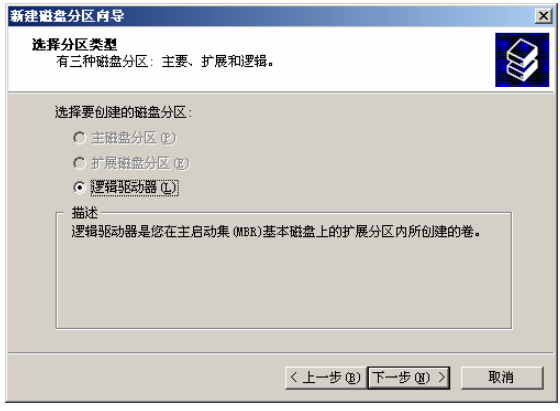

图 4.8　选择分区类型—逻辑驱动器

（2）单击“下一步”按钮，弹出“指定分区大小”对话框，如图 4.7 所示，其单位是 MB，如果要分配 20GB 空间，可以输入 20 000。

（3）单击“下一步”按钮，弹出“指定驱动器号和路径”对话框，选择默认的“D:”盘符。

（4）单击“下一步”按钮，弹出“格式化分区”对话框，选择合适的文件系统来格式化分区，从安全角度考虑，一般使用 NTFS 文件系统。

- “卷标”是磁盘分区的名字，可以根据分区的作用来命名，例如，可以将“D:”盘的卷标设为“应用软件”。
- 执行快速格式化：选择此项时，系统只是重新创建 FAT、FAT32 或 NTFS 格式，不会检查是否有坏扇区，同时磁盘内原有文件不会真正地被删除。
- 启动文件及文件夹压缩：选此项，可将该磁盘设为“压缩磁盘”，以后添加到该磁盘分区中的文件及文件夹都会被自动压缩。

（5）单击“下一步”按钮，系统自动创建逻辑驱动器，并进行格式化操作。格式化完成后，刚才创建的逻辑驱动器就加入到“磁盘管理”窗口中。

（6）其他两个逻辑驱动器的创建方法同前。

步骤 5：创建主分区

一个基本磁盘内最多可以有 4 个主磁盘分区。创建主磁盘分区的步骤如下：

（1）启动“磁盘管理”程序，选取一块未指派的磁盘空间，这里我们选择“磁盘 2”。右击该空间，在弹出的菜单中选择“新建磁盘分区”选项，弹出“欢迎使用新建磁盘分区向导”对话框。

（2）单击“下一步”按钮，弹出“选择分区类型”对话框，如图 4.6 所示，选择“主磁盘分区”单选选项。

（3）单击“下一步”按钮，弹出“指定分区大小”对话框，输入该主磁盘分区的容量。

（4）单击“下一步”按钮，弹出“指定驱动器号和路径”对话框，选择默认的“D:”盘符。

（5）单击“下一步”按钮，弹出“格式化分区”对话框，选择合适的文件系统来格式化分区，从安全角度考虑，一般使用 NTFS 文件系统。

（6）单击“下一步”按钮，系统自动创建主分区，并进行格式化操作。格式化完成后，刚才创建的主分区就加入到“磁盘管理”窗口中。

步骤 6：FAT和NTFS文件系统的转换

如果需要将文件系统由原来的 FAT32 格式转换为 NTFS 格式，并且不希望数据丢失，可以利用命令“convert 盘符/FS:NTFS”，将特定分区由 FAT32 转换为 NTFS。

例如，将 F 盘由 FAT32 格式转换为 NTFS 格式，命令为：

```
convert F:/FS:NTFS
```

步骤 7：磁盘基本管理

（1）更改驱动器号和路径。一般情况下，绝对不能随意更改驱动器号，以防应用程序找不到所需的数据。正在使用的系统卷与引导卷的驱动器号无法改变。

Windows Server 2003 中可以将一个分区映射为一个文件夹，这样所有保存在该文件夹中的文件事实上都保存在分区上。下面介绍如何将光驱映射到“D:\光驱文件夹”中。

① 打开“磁盘管理”窗口，右击“光驱”，打开“更改 G:（光驱）驱动器号和路径”对话框，如图 4.9 所示。

② 单击“添加”按钮，弹出“添加驱动器号或路径”对话框，如图 4.10 所示，在“装入以下空白 NTFS 文件夹中”文本框中输入“D:\光驱文件夹”或单击“浏览”按钮进行选择。单击“确定”按钮，完成操作。这时在资源管理器中可以看到光驱在 D 盘下以文件夹的形式出现。

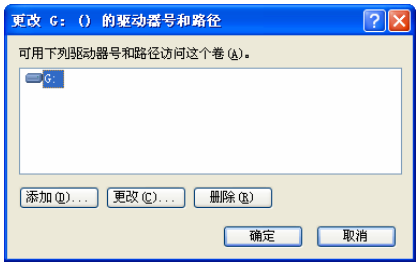

图 4.9　更改 G:（光驱）驱动器号和路径

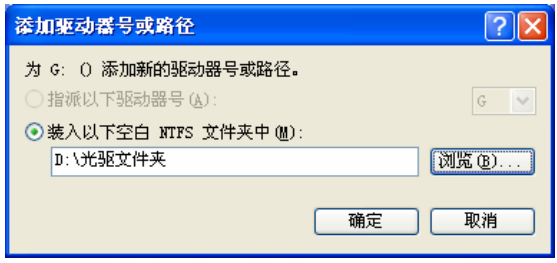

图 4.10　添加驱动器号或路径

（2）重新格式化分区。打开“磁盘管理”窗口，右击要重新格式化的分区，选择“格式化”选项，弹出“格式化”对话框，如图 4.11 所示。

设置卷标和文件系统，为了提高速度，可以选中“执行快速格式化”复选框。

格式化时也可以选择文件系统为 FAT32 还是 NTFS。

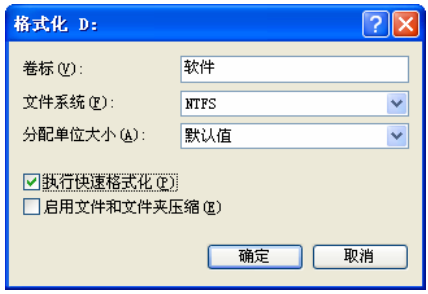

图 4.11　格式化

（3）删除逻辑驱动器和磁盘分区。在 Windows Server 2003 的磁盘管理工具中，如果要改变某个分区或逻辑驱动器的大小，必须先删除该分区或逻辑驱动器，然后重新建立分区或逻辑驱动器。

在“磁盘管理”窗口中，右击要删除的磁盘分区或逻辑驱动器，选择“删除磁盘分区”或“删除逻辑驱动器”，然后在提示对话框中选择“是”就可以了。

步骤 8：更改主分区的大小

操作系统安装完成后，发现计算机硬盘 C 区空间分配的太小，造成系统速度变慢，于是希望把 C 区空间变大。

Windows 操作系统提供的磁盘管理工具只能删除分区，再重新划分分区大小。这样会造成丢失数据，并且要求重新安装操作系统。

在这种情况下，可以使用专门的分区工具软件来达到更改主分区大小的目的，它们的功能比 Windows 的磁盘管理工具更加强大，可以在不破坏原分区数据的情况下，改变分区大小。其中最常用的是 Symantec 公司的 PowerQuest PartitionMagic 软件。

PowerQuest PartitionMagic 是一个优秀的硬盘分区管理工具。该工具可以在不损失硬盘中已有数据的前提下对硬盘进行重新分区、格式化分区、复制分区、移动分区、隐藏/重现分区、从任意分区中引导系统、转换分区（如 FAT 在 FAT32 之间转换）结构属性等。

（1）运行 PowerQuest PartitionMagic，打开 PowerQuest PartitionMagic 程序窗口，如图 4.12

所示。

（2）单击左边区域的“调整一个分区的容量”，弹出“调整分区容量”对话框，单击“下一步”按钮，弹出“选择分区”对话框，如图 4.13 所示。选择要增加容量的分区，在这里选择 C:分区。

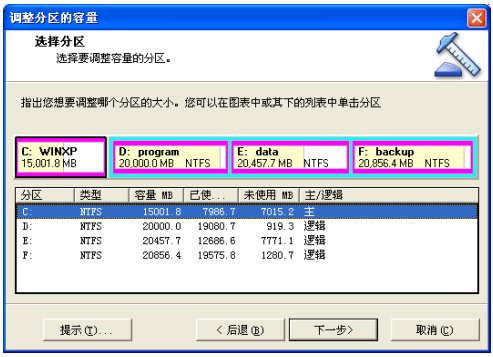

图 4.12　PowerQuest PartitionMagic 程序窗口

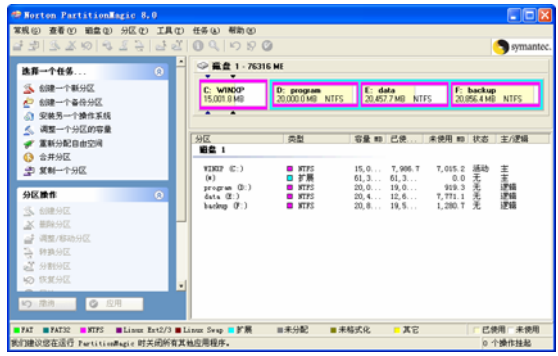

图 4.13　“调整分区容量”对话框

（3）单击“下一步”按钮，弹出“指定新建分区的容量”对话框，如图 4.14 所示。在“分区的新容量”栏中输入新的容量。

（4）单击“下一步”按钮，弹出“减少哪一个分区的空间”对话框，如图 4.15 所示。选择要挪动的那些容量来自哪个区（也就是减少这个区的容量，来给希望增加容量的区增容），在这里选择“E:”。

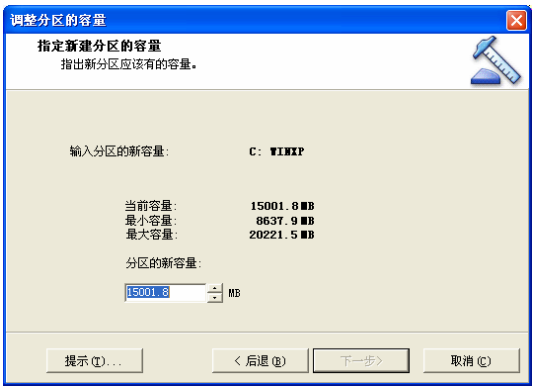

图 4.14　“指定新建分区的容量”对话框

图 4.15　“减少哪一个分区的空间”对话框

（5）单击“下一步”按钮，弹出“确定调整分区容量”对话框，如图 4.16 所示。可以看到改变分区容量大小前后的对比。

（6）单击“完成”按钮。

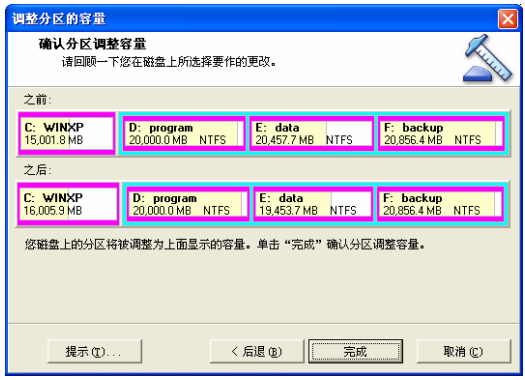

图 4.16 “确认分区调整容量”对话框

4.3.2 任务 2：动态磁盘的管理

1．工作任务

公司的客户购买了一台新计算机，公司要求你负责为客户安装操作系统和软件，并使用动态磁盘方式进行管理。

2．实施过程

步骤 1：基本磁盘升级为动态磁盘

在默认状态下磁盘的类型是基本磁盘，我们必须使用 Windows Server 2003 的“磁盘管理”将指定的磁盘由基本磁盘模式升级到动态磁盘模式。

另外，由于基本磁盘升级到动态磁盘，需要注意以下问题：

（1）只有属于 Administrator 或 Backup Operators 组的成员才有权进行磁盘转换操作；

（2）在转换之前，应该关闭所有正在运行的程序；

（3）当基本磁盘升级到动态磁盘后，基本磁盘上的现有分区将转换为动态磁盘上的简单卷；

（4）若要将动态磁盘转换为基本磁盘，必须先删除磁盘上的所有动态卷，然后再转换，这会丢失磁盘上的所有数据；

（5）升级到动态磁盘后，只有 Windows 2000/XP Professional/Server 2003 才能对动态磁盘进行本地访问；

（6）如果升级的磁盘包括当前的操作系统或者引导文件，则升级需要重新启动以后才能完成。

注意 将基本磁盘升级为动态磁盘具有一定的危险性，一旦升级失败有可能造成磁盘上的数据全部丢失。

将基本磁盘升级到动态磁盘，可参照如下步骤。

（1）关闭所有正在运行的应用程序，打开“计算机管理”窗口中的“磁盘管理”。右击要升级的基本磁盘，在弹出菜单中选择“转换到动态磁盘”选项。

（2）打开“转换为动态磁盘”对话框，如图 4.17 所示，可以选择多个磁盘一起升级。

（3）单击“确定”按钮。打开“要转换的磁盘”对话框，如图 4.18 所示，单击“转换”按钮即可。

图 4.17　“转换为动态磁盘”对话框

图 4.18　“要转换的磁盘”对话框

升级完成后，在管理窗口中可以看到磁盘的类型改为动态。

步骤 2：创建简单卷

简单卷只使用一个物理磁盘上的可用空间，可以是单个区域，也可以是多个不连续的区域。简单卷可以在同一物理磁盘内扩展空间，如果跨越多个磁盘扩展简单卷，则该卷就成了跨区卷。简单卷可以被格式化为 FAT32 或 NTFS 文件系统。

（1）在“磁盘管理”窗口中，右击要升级的磁盘，选择“新建卷”选项，弹出“新建卷向导”对话框，如图 4.19 所示，选择“简单卷”单选框。

（2）单击“下一步”按钮，弹出“选择磁盘”对话框，如图 4.20 所示。选择将简单卷建立在哪个磁盘上，并设置卷的大小。

图 4.19　“选择卷类型”对话框

图 4.20　“选择磁盘”对话框

（3）单击“下一步”按钮，弹出“指派驱动器号和路径”对话框，为该卷指派一个驱动器号。单击“下一步”按钮，弹出“卷区格式化”对话框，选择合适的文件系统和卷标。单击“下一步”按钮，单击“完成”按钮，系统将对该卷格式化。

步骤 3：创建扩展卷

如果要建立的简单卷的空间不能满足需求，可将邻近的未指派空间加入到该简单卷中。但只有 NTFS 文件系统格式化的简单卷才可以被扩展。如果将简单卷扩展到其他的动态磁盘上，就成了跨区卷。

在 NTFS 文件系统的简单卷上右击，选择“扩展卷”选项，打开“扩展卷向导”对话框。单击“下一步”按钮，弹出“选择磁盘”对话框，在其中选择要扩展多少空间。单击“下一

步”按钮，单击“完成”按钮。

步骤 4：创建跨区卷

公司的服务器上有若干块硬盘，单块硬盘最大只有 80GB，而这时希望在服务器上创建一个大小为 100GB 的卷，这时候就可以创建一个跨区卷。跨区卷由多个磁盘上的可用空间组成，它们合并为一个逻辑卷。

创建跨区卷的步骤如下：

（1）右击动态磁盘的未分配空间，选择“新建卷”选项，打开“新建卷向导”对话框。

（2）单击“下一步”按钮，弹出“选择卷类型”对话框，选择“跨区卷”单选框。

（3）单击“下一步”按钮，弹出“选择磁盘”对话框，选择可用的动态磁盘“添加”到右侧列表中，并指定每个磁盘上使用的容量大小。如跨区卷在磁盘 0 上占用了 40GB，在磁盘 1 上占用了 60GB，卷大小总数为 100GB。

（4）单击“下一步”按钮，弹出“指派驱动器号和路径”对话框，为该跨区卷指派一个驱动器号。单击“下一步”按钮，弹出“卷区格式化”对话框，选择合适的文件系统和卷标。单击“完成”按钮。

跨区卷有如下特性：

① 组成跨区卷的磁盘可以是 2～32 个；

② 组成跨区卷的每个磁盘所使用的空间可以不同；

③ 跨区卷不能是系统卷和引导卷；

④ 在跨区卷中存储数据时，先存到跨区卷占用的第一个磁盘空间，空间用尽后，再存到第二个磁盘的空间；

⑤ 跨区卷无容错功能，如果成员磁盘中的任何一个发生故障，整个跨区卷的数据都会丢失。

步骤 5：创建带区卷

由于公司的文件服务器经常要读写大量的数据，因此希望能尽量提高读写磁盘的效率，这时可以在服务器上创建带区卷。

带区卷同样使用至少两块物理磁盘的空间来存储数据，但带区卷在每个成员磁盘上的容量大小相同，且数据交替平均存储于各个磁盘上，如图 4.21 所示。带区卷数据写入时，以 64KB 为单元平均写到每个磁盘上，先将第一块硬盘的第一个单元写满，再写第二块硬盘的第一单元；当最后一块硬盘的第一单元写满后，再回到第一块硬盘的第二单元，一次写入数据。由于带区卷允许并发的 I/O 操作，可以在所有的成员磁盘上同时执行读写，因此，带区卷可以极大地提高系统读写的性能。

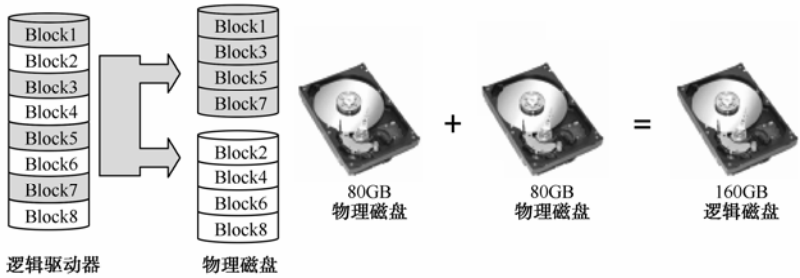

图 4.21　带区卷

创建带区卷的步骤如下：

（1）右击动态磁盘的未分配空间，选择“新建卷”选项，打开“新建卷向导”对话框。

（2）单击“下一步”按钮，弹出“选择卷类型”对话框，选择“带区卷”单选框。

（3）单击“下一步”按钮，弹出“选择磁盘”对话框，选择可用的动态磁盘和需要的容量。可以选择单个磁盘占用了 1 500MB，卷大小总数为 3 000MB。

（4）单击“下一步”按钮，弹出“指派驱动器号和路径”对话框，为该带区卷指派一个驱动器号。单击“下一步”按钮，弹出“卷区格式化”对话框，选择合适的文件系统和卷标。单击“完成”按钮。

同样，带区卷不具备容错功能，任何一个成员磁盘损坏后，整个带区卷都将不能使用。带区卷不能扩展容量，带区卷不能是系统卷和引导卷。

步骤 6：创建镜像卷

公司服务器上的某些数据非常重要，希望能够有一种磁盘容错机制，使得即使某块磁盘发生故障，数据也不会丢失。这时可以考虑用镜像卷来保存这些重要数据。

镜像卷是一种容错卷，它一般由两个物理磁盘上的空间组成。写入数据时，数据会复制为两份并同时写到两块磁盘上，如图 4.22 所示。如果其中一块磁盘发生故障，还可以从剩下的一块磁盘中访问数据，提高了数据的安全性。

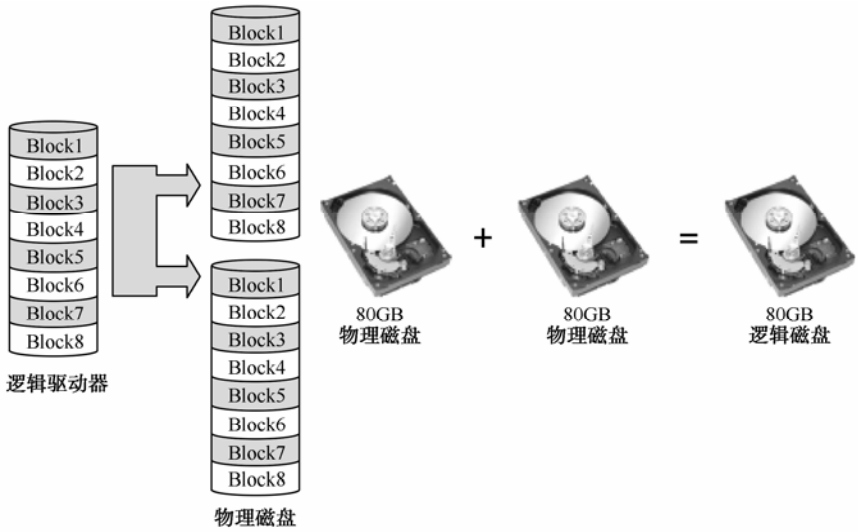

图 4.22　镜像卷

创建镜像卷的步骤如下。

（1）右击动态磁盘的未分配空间，选择“新建卷”选项，打开“新建卷向导”对话框。

（2）单击“下一步”按钮，弹出“选择卷类型”对话框，选择“镜像卷”单选框。

（3）单击“下一步”按钮，弹出“选择磁盘”对话框，选择可用的动态磁盘和需要的容量。如果镜像卷使用磁盘 1 和磁盘 2，并指定单块磁盘的容量大小为 1 000MB，则卷大小总数为 1 000MB。

（4）单击“下一步”按钮，弹出“指派驱动器号和路径”对话框，为该镜像卷指派一个驱动器号。单击“下一步”按钮，弹出“卷区格式化”对话框，选择合适的文件系统和卷标。

单击“完成”按钮。

也可以直接为以前创建的简单卷添加镜像。在要镜像的简单卷上右击，选择“添加镜像”选项，然后按向导提示进行操作即可。

如果镜像卷中的一个成员发生了故障，则需要先中断镜像或删除镜像。

中断镜像：在镜像卷上右击，选择“中断镜像卷”选项。中断之后，镜像卷中的成员都会独立成简单卷，且其中数据都被保留。

删除镜像：在镜像卷上右击，选择“删除镜像”选项。删除了镜像的那个成员上的数据将会被删除，并且释放空间为未指派空间；另一成员独立成简单卷。

镜像卷有如下特性：

① 镜像卷要求两个成员磁盘上的空间大小相同；

② 系统卷或引导卷可以作为镜像卷；

③ 不支持扩展容量；

④ 写入数据的时间较长，但读取数据时效率较高；

⑤ 磁盘利用率低，只有 50%。

步骤 7：创建RAID-5 卷

镜像卷虽然提供了较强的容错能力，但它的磁盘空间利用率低，存储成本较高。为了提供磁盘的利用率，可以采用 RAID-5 卷。

RAID-5 卷的数据分布于由三个或更多磁盘组成的磁盘阵列中，写入数据时首先要计算数据的奇偶校验；把数据和相对应的奇偶校验信息存储到组成 RAID-5 卷的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当 RAID-5 的一个磁盘数据发生损坏后，可以利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。如图 4.23 所示。

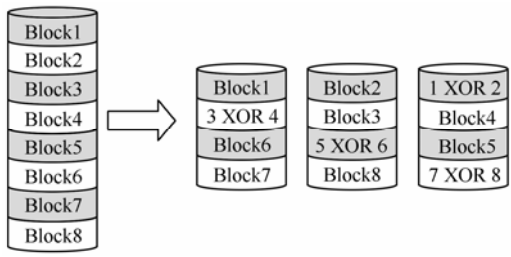

图 4.23　RAID-5 卷

（1）创建 RAID-5 卷。创建 RAID-5 卷的步骤如下：

① 右击动态磁盘的未分配空间，选择“新建卷”选项，打开“新建卷向导”对话框；

② 单击“下一步”按钮，弹出“选择卷类型”对话框，选择“RAID-5 卷”单选框；

③ 单击“下一步”按钮，弹出“选择磁盘”对话框，选择可用的动态磁盘和需要的容量。至少需要加入三块动态磁盘，且最后的实际容量是加入磁盘总容量的 2/3；

④ 单击“下一步”按钮，弹出“指派驱动器号和路径”对话框，为该 RAID-5 卷指派一个驱动器号。单击“下一步”按钮，弹出“卷区格式化”对话框，选择合适的文件系统和卷标。单击“完成”按钮。

（2）修复 RAID-5 卷。在使用 RAID-5 卷的过程中，如果三块硬盘中的任意一块硬盘损坏，都不会影响用户对整体数据的访问，可以对其进行修复。

对 RAID-5 卷的修复分为不更换原磁盘的修复和更换原磁盘的修复。

① 如果磁盘没有发生物理故障，则修复起来比较简单。首先确认发生故障的磁盘是否已经和计算机正确连接，然后打开磁盘管理窗口，在状态显示为“丢失”、“脱机”或“联机错误”的动态磁盘上右击，选择“重新激活磁盘”选项即可。

② 如果是磁盘出现物理故障，首先要更换一块相同型号的硬盘，并将该磁盘设置为动态磁盘；然后打开磁盘管理窗口，用鼠标在发生故障的 RAID-5 卷上右击，选择“修复卷”选项即可。打开“修复卷”对话框，系统会自动搜索到一个新的硬盘来替代坏的硬盘，只需要单击“确定”按钮，系统会自动去创建原来丢失的磁盘空间，同时自动恢复数据。

4.3.3 任务 3：管理磁盘配额

1．工作任务

公司的客户购买了一台新计算机，公司要求你负责为客户安装操作系统和软件，进行磁盘配额管理工作。

2．相关知识

Windows Server 2003 提供了磁盘配额功能以限制用户对磁盘空间的无限使用。系统管理员通过磁盘配额管理器，设置用户可以使用的磁盘空间数量。当用户对受保护的磁盘卷进行写入操作时，磁盘配额管理器会根据系统管理员设置的条件，监视用户的写入操作；如果发现用户接近或超过限额时，就会发出警告或者阻止该用户对卷的写入。

Windows Server 2003 的磁盘配额管理是基于用户和卷的，限额的磁盘是 Windows 卷，而不是各个物理硬盘。要在卷上启用磁盘配额，该卷的文件系统必须是 NTFS 格式。

3．实施过程

步骤 1：启用磁盘配额

（1）在需要启用磁盘配额的卷上右击，选择“属性”选项，打开“卷的属性”对话框。

（2）选择“配额”选项卡，选中“启用配额管理”复选框，设置配额限制和警告等级，如图 4.24 所示。

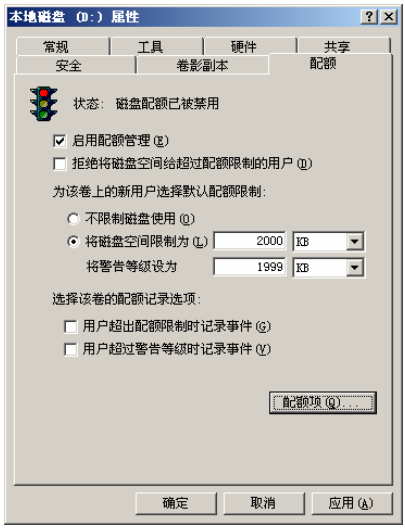

图 4.24 “配额”选项卡

- 拒绝将磁盘空间分给超过配额限制的用户：当某个用户占用的磁盘空间达到了配额的限制时，就不能再使用新的磁盘空间，Windows 会提示用户“磁盘空间不足”。
- 不限制磁盘使用：管理员不限制用户对卷空间的使用，只是对用户的使用情况进行跟踪。
- 将磁盘空间限制为：可以输入限制用户使用的磁盘空间的数量和单位，这是所有用户的默认值。
- 将警告等级设为：当用户使用的磁盘空间超过警告等级时，系统会及时地给用户警告。警告等级的设置应该不大于磁盘配额的限制。
- 用户超出配额限制时记录事件：表示用户使用的磁盘空间超过配额限制时，系统会在本地计算机的日志文件中记录该事件。

- 用户超过警告等级时记录事件：表示用户使用的磁盘空间超过警告等级时，系统会在本地计算机的日志文件中记录该事件。

（3）设置完成后，单击“确定”按钮，系统扫描该卷，为使用该卷的用户创建磁盘配额项。如果有超出配额限制的用户，不会记录到日志中，只是在用户再次存储信息时拒绝其使用。

只有 Administrator 组的用户有权启用磁盘配额，而且 Administrator 组的用户不受磁盘配额的限制。磁盘配额限制的大小与卷本身的大小无关，例如，卷的大小是 2 000MB，有 100 个用户要使用该卷，可以为每个用户设置磁盘配额为 100MB。

在卷上启用磁盘配额后，普通用户登录进入系统时，看到的该卷的大小是其被限制使用的空间的大小。

步骤 2：调整磁盘配额限制和警告等级

除了可以为所有用户指定默认的磁盘配额外，还可以单独为某个用户或用户组指定磁盘配额项，以满足某些用户的特定需求。

（1）在卷的“配额”选项卡中，单击“配额项”按钮，打开新加卷的配额项对话框，如图 4.25 所示。

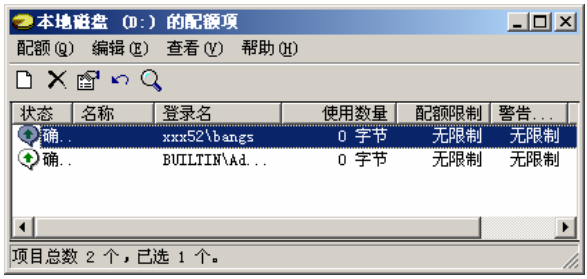

图 4.25　新加卷的配额项

（2）在列表中右击用户“bangs”，选择“属性”选项，打开“bangs 的配额设置”对话框，如图 4.26 所示。为用户“bangs”重新设置磁盘空间限制和警告等级等。

步骤 3：删除磁盘配额项

某用户在服务器的卷上可能创建了很多文件，如果要求把该用户在该卷上的所有文件和文件夹全部移动到其他卷上，或者当该用户辞职，要求删除该用户的所有文件时，可以使用删除该用户的磁盘配额项的方法来进行。

在图 4.25 所示的“新加卷的配额项”对话框中，选择“配额”菜单中的“删除配额项…”选项，删除该用户的磁盘配额。

步骤 4：导入和导出磁盘配额项目

公司有两台文件服务器，其共享的 NTFS 卷要求实施相同的磁盘配额限制。这时管理员可以使用磁盘配额的导入/导出功能，将一个卷的配额项设置复制到另一个卷中。

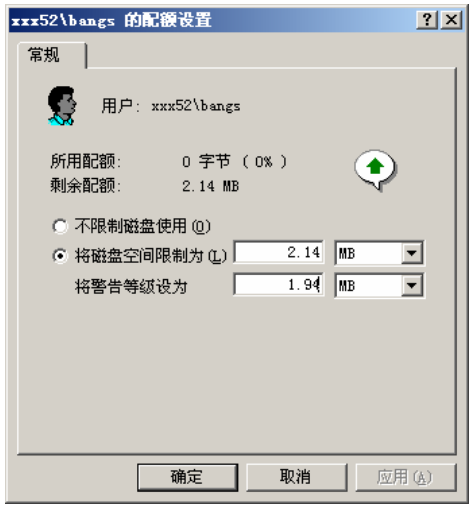

图 4.26　用户 bangs 的配额设置

（1）首先在一个卷上设置好磁盘配额项，然后打开其“配额项”窗口。

（2）选中要导出的配额项。然后打开“配置”菜单，选择“导出”选项。打开保存文件的对话框，可以将当前卷中选中的磁盘配额项设置保存在文件中。

（3）将保存的文件复制到另一台服务器上。打开要设置磁盘配额的卷的“配额项”窗口。

（4）打开“配置”菜单，选择“导入”选项。在“打开”对话框中，找到刚才保存的文件，单击“打开”按钮即可。

习　题

一、填空题

1．在 Windows Server 2003 服务器的磁盘管理中，将磁盘类型分为基本磁盘和_____。

2．在 NTFS 卷上，可以通过_____ 管理来限制用户使用的磁盘空间大小。

二、选择题

1．一个基本磁盘最多有（　　）个主分区。

A．1　　B．2　　C．3　　D．4

2．一个基本磁盘最多有（　　）个扩展区。

A．1　　B．2　　C．3　　D．4

3．以下所有动态磁盘卷类型中，运行速度最快的卷是（　　）。

A．简单卷　　B．带区卷　　C．镜像卷　　D．RAID-5 卷

4．在基本磁盘管理中，扩展分区不能用一个具体的驱动器盘符表示，必须在其中划分（　　）之后才可以使用。

A．主分区　　B．格式化　　C．逻辑驱动器　　D．卷

5．要启用磁盘配额管理，Windows Server 2003 驱动器必须使用（　　）文件系统。

A．FAT16 或 FAT32　　B．只使用 FAT32

C．NTFS 或 FAT32　　D．只使用 NTFS

三、思考题

1．基本磁盘和动态磁盘有哪些区别？

2．为什么带区卷比跨区卷能提供更好的性能？

3. 什么是磁盘配额？

四、实训题

1．在动态磁盘上创建带区卷。

2．对磁盘“D:”做磁盘配额操作，所有用户默认的磁盘配额限制为 50MB，其中设置用户 user1 的磁盘配额空间为 100MB。

项目 5　活动目录和域的组建

5.1　项目内容

1．项目目的

通过安装活动目录，理解活动目录和域的关系，了解域、域树和域林的概念，并掌握域控制器的安装和配置，以及成员服务器的设置。

2．项目任务

某公司组建了单位内部的办公网络，该局域网是一个基于工作组的对等网。近期公司的发展很快，新增了许多员工，计算机用户数量激增，网络的管理和安全都出现了问题，这时考虑将基于工作组的网络升级为基于域的网络，现在需要将一台计算机升级为域控制器，并将其他所有计算机加入到域成为成员服务器。

3．任务目标

① 学会规划和安装局域网中的活动目录；
② 学会在 Windows Server 2003 中创建域；
③ 学会在 Windows Server 2003 中添加和管理各种域服务器；
④ 学会将局域网中的计算机加入在 Windows Server 2003 系统下的域服务器中。

5.2　相关知识

5.2.1　域

在主从式网络中，资源集中存放在一台或几台服务器上，如果只有一台服务器，管理比较简单，在服务器上为每一个用户建立一个账户即可，用户只需要登录该服务器就可以使用服务器中的资源。然而资源如果分布在多台服务器上，如图 5.1 所示，就需要在每台服务器上（共 M 台）分别为每一个用户（共 N 个）建立一个账户（共 M×N 个），用户则需要在每台服务器上登录。那么能否解决用户多次登录不同的服务器，以及在不同的服务器上为同一用户多次创建账户的问题呢？这时就出现了域模型。

如图 5.2 所示，服务器和用户的计算机都在同一个域中，用户在域中只要拥有一个账号，只需要在域中用该账户登录一次就可以访问域中任何一台服务器上的资源。在每一台存放资源的服务器上并不需要为每一用户创建账户，而只需要把资源的访问权限分配给用户在域中的账户即可。

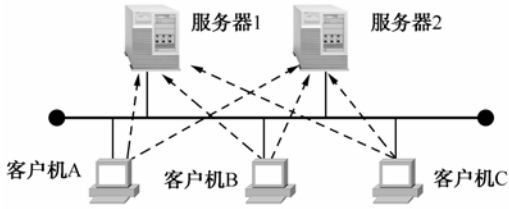

图 5.1　资源分布在多台服务器上

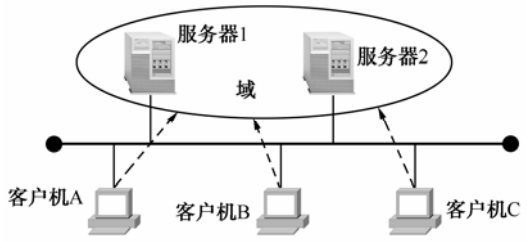

图 5.2　域的模式

在图 5.2 所示的域中有多台服务器，这时域中的账户信息（如用户名和密码等）放在一台称为域控制器（Domain Controller，DC）的服务器上。在一个域中，可以选定一台或多台服务器作为域控制器。此时每个域控制器是平等的，每个域控制器上都有所在域的全部用户的信息，其他不是域控制器的服务器仅仅提供资源。

随着网络的发展，企业网络越来越大。当网络有上万个用户甚至更多时，图 5.2 中的域控制器存放的用户数量将很大，并且如果用户频繁登录，对作为域控制器的服务器的性能要求也越来越高，可能因此而不堪重负，并且用户账户的管理更是无法由一个部门来解决。这时需要分成多个域，每个域的规模都控制在一定的范围内，各个域分别管理自己的账户，如图 5.3 所示。

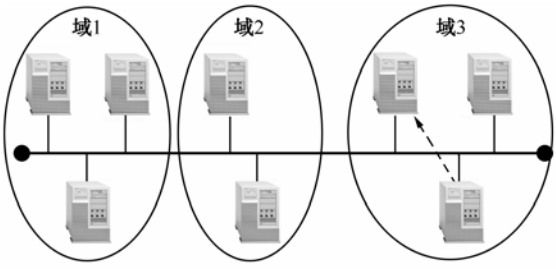

图 5.3　网络划分成多个域

在图 5.3 中，域 1 中的用户登录后可以访问域 1 和域 3 中的服务器上的资源，域 2 的用户可以访问域 1 中的服务器上的资源；但域 1 的用户不能访问域 2 中的服务器上的资源，域 2 的用户也不能访问域 1 中的服务器上的资源。

为了解决用户跨域访问资源的问题，可以在域之间引入信任。信任关系有单向和双向两种。如图 5.4（a）是单向的信任关系，箭头指向被信任的域，即 A 域信任 B 域，A 称为信任域（Trusting Domain），B 称为被信任域（Trusted Domain），因此 B 域的用户可以访问 A 域中的资源。图 5.4（b）是双向的信任关系，A 域信任 B 域，同时 B 域信任 A 域，因此 A 域中的用户可以访问 B 域中的资源，反之亦然。有了信任关系，在图 5.3 中，如果域 1 的用户要访问域 2 中的资源，只要让域 2 信任域 1 就可以了。

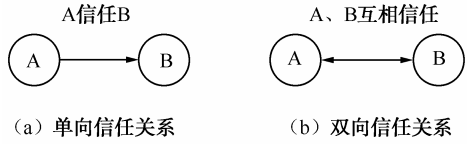

图 5.4　信任关系

信任关系有可传递和不可传递之分。A 信任 B，B 又信任 C，如果信任关系是可传递的，那么 A 就信任 C；如果信任关系是不可传递的，那么 A 就不信任 C。

5.2.2 域树

在一个企业中可能会有分布在各地的分公司，分公司下又有各种部门存在，因此企业可能有数万个用户、成百上千的服务器以及上百个域，资源的访问常常可能跨越多个域。在 Windows NT 4.0 时代，域和域之间的信任关系是不可传递的，如果一个网络中有很多域，要互相跨域访问资源，必须创建多个双向信任关系。如果有 n 个域，那么所需的双向信任关系的数量为 $n(n-1)/2$，如图 5.5 所示。

之所以会这样，是因为 A、B、C、D、E 域被看成是独立的域，所以信任关系被看成不可传递的，而实际上 A、B、C、D、E 域都是在同一企业中，很可能 B 是 A 的主管单位，C 又是 B 的主管单位。从 Windows Server 2000 起，域树开始出现，如图 5.6 所示。

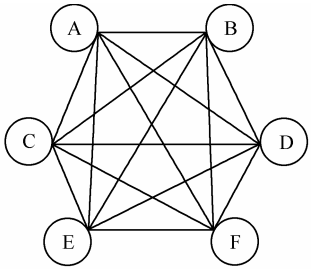

图 5.5　多个域的资源互访需要多个信任关系

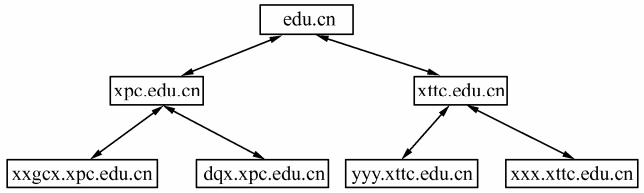

图 5.6　域树

图 5.6 的域树中的域以树的形式出现，最上层的域名为 edu.cn，是这个域树的根域。根域下有两个子域：xpc.edu.cn 和 xttc.edu.cn。xpc.edu.cn 和 xttc.edu.cn 子域下又有自己的子域。在域树中，父域和子域的信任关系是双向可传递的，因此域树中的一个域隐含地信任域树中所有的域。图 5.6 中共有 7 个域，所有域相互信任也只需要 6 个信任关系。

5.2.3 域林

域树中，域的名字是从父域派生出来的。在一个域树中，域的名字是连续的。如果某个企业同时拥有 edu.cn 和 gov.cn 两个域名，这时就需要单独创建两个域树，如图 5.7 所示，这两个域树就构成了域林。在同一域林中的域树的信任关系也是双向可传递的。

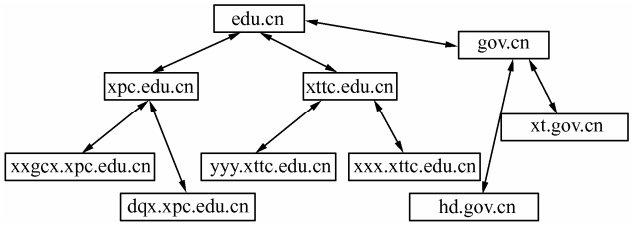

图 5.7　域林

5.2.4 信任关系

信任是域之间建立的关系，它可使一个域中的用户由处在另一个域中的域控制器来进行验证。Windows Server 2003 中域之间的信任关系建立在 Kerberos 安全协议上，Kerberos 信任是可传递的、分层次和结构的。Windows Server 2003 域树和域林中的所有信任都是可传递的、双向信任的，因此，信任关系中的两个域都是相互受信任的。如图 5.8 所示，如果域 A 信任

域 B，并且域 B 信任域 C，则域 C 中的用户（授予适当权限时）可以访问域 A 中的资源。只有域管理员组的成员可以管理信任关系。

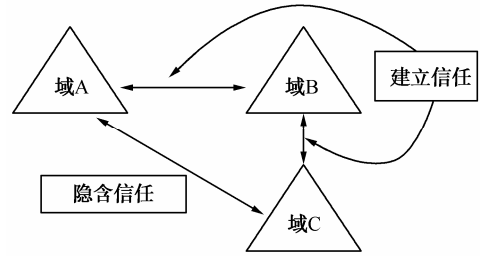

图 5.8　一个域树以其信任关系表示

1．信任协议

运行 Windows Server 2003 的域控制器使用 Kerberos V5 和 NTLM 两种协议之一来验证用户和应用程序。Kerberos V5 协议是运行 Windows 计算机的默认协议。如果事务中所涉及的任何计算机都不支持 Kerberos V5，则将使用 NTLM 协议。

2．信任类型

域和域之间的通信是通过信任发生的。信任是为了使一个域中的用户访问另一个域中的资源而必须存在的身份验证管道。使用“Active Directory 安装向导”时，将会创建两个默认信任。默认情况下，当使用“Active Directory 安装向导”在域树或域林的根域中添加新域时，系统会自动创建双向的可传递信任。表 5.1 所列为两种默认信任类型。

表 5.1　两种默认信任类型

信任类型	传递性	方向	说　明
父子	可传递	双向	默认情况下，当在现有域树中添加新的子域时，将建立一个新的父子信任。来自从属域的身份验证请求将通过其父域向上传递到信任域中
树根	可传递	双向	默认情况下，当在现有域林中添加新的域树时，将建立一个新的树根信任

使用“新建信任向导”可创建另外 4 种类型的信任，见表 5.2。

表 5.2　其他信任类型

信任类型	传递性	方向	说　明
外部	不可传递	单向或双向	使用外部信任可访问域中的资源，或单独（未经林信任连接）的林内某个域中的资源
域树	可传递或不可传递	单向或双向	使用域树信任可建立非 Windows Kerberos 域树和 Windows Server 2003 域之间的信任关系
域林	可传递	单向或双向	使用域林信任可在各个域林之间共享资源。如果域林信任是双向信任，则任一个域林中的身份验证请求都可以到达另一个域林
快捷	可传递	单向或双向	使用快捷信任可改善 Windows Server 2003 域林内的两个域之间的用户登录时间

3．委托

委托是活动目录最重要的安全特性之一，委托使得较高级的管理员对个人或组授予对容

器和子树特定的管理权。这样就通过取消大部分用户组的权利而消除了对“域管理员”的需求。

4．继承

继承是授予用户或组权限的对象自由访问控制列表（DACL）中的一个项目，也是对象的系统访问控制列表（SACL）中的项目，该列表指定用户或组要审核的安全事件，访问控制项也被称为 ACE。继承使得一个给定的 ACE 可以从它应用的容器传播到其所有子孙的容器。继承可以与委托相结合，从而保证对目录中整个子树的某一单一操作的管理权。

5．复制

活动目录提供多主版本复制。多主版本复制意味着给定分区的所有复制都是可写的，这就使得给定分区的任意复制的更新都可以完成。活动目录复制系统将一个给定复制的改变传递给所有其他复制。复制是自动且透明的。

6．双向可传递的信任

当一个域加入一个 Windows Server 2003 域树中时，在加入域与该树中父代之间的双向可传递信任关系就自动建立了。由于信任是双向的和可传递的，因此域成员之间的其他附加信任关系是不需要的。

5.2.5　活动目录

1．活动目录的概念

微软的活动目录（Active Directory，AD）是一种存放信息的方式。在域控制器上存放有域中所有用户、组、计算机等的信息，域控制器把这些信息存放在活动目录中，因此活动目录实际上就是一个特殊的数据库。一台域中的服务器如果安装了活动目录，它就成为域控制器。域控制器就是安装了活动目录的服务器。

活动目录是 Windows Server 2003 系统中提供的目录服务，用于存储网络上各种对象的相关信息，以便管理员查找和使用。目录服务是一种提供了按层次结构组织的信息，然后按名称关联检索信息的服务方式。

活动目录存储着本网络上各种对象的相关信息，并使用一种易于用户查找及使用的结构化的数据存储方法来组织和保存数据。在整个目录中，通过登录验证和目录中对象的访问控制，将安全性集成到活动目录中。通过一次登录，管理员可以管理整个网络中的目录数据和单位，而且获得授权的网络用户可以访问网络上所有的资源。

2．活动目录和DNS

在 TCP/IP 网络中，DNS 是用来解决计算机名字和 IP 地址的映射关系的。Windows Server 2003 的活动目录和 DNS 是紧密不可分的，它使用 DNS 服务器来登记域控制器的 IP 地址、各种资源的定位等，因此在一个域林中至少要有一个 DNS 服务器存在。Windows Server 2003 中域也是采用 DNS 的格式来命名的。

3．活动目录中的组织单元

（1）对象：在 Windows Server 2003 的活动目录中存放着各种对象的信息，这些对象包括用户、计算机、打印机和组等。每个对象都有自己的属性及属性值。对象实际上就是属性的集合，例如，一个名为 ds0523 的账户就是一个对象类的具体实例，该对象类有姓、名、电话

号码和地址等属性。

（2）组织单元：组织单元（Organization Unit，OU）用来组织对象，如账户、打印机、服务器、组、应用程序等，组织单元把这些对象按逻辑进行分组，便于管理、查找、授权和访问。组织单元是类型为容器的对象，容器是可以包含其他对象的对象。但组织单元是在某个域下的，不能包含域。组织单元有许多划分方法，也可以根据地理位置进行划分。

4．全局编录

有了域林之后，同一域林中的域控制器有一个活动目录，这个活动目录是分散存放在各个域的域控制器上的，每个域中的域控制器存有该域的对象的信息。如果一个域的用户要访问另一个域中的资源，那么这个用户要能够查找到另一个域中的资源才行。为了让每一位用户都能够快速查找到另一个域中的对象，微软设计了全局编录（Global Catalog，GC）。全局编录包含了整个活动目录中每一个对象的最重要的属性（即部分属性，而不是全部），这使得用户或应用程序即使不知道对象位于哪个域内，也可以迅速找到被访问的对象。

5．域控制器、成员服务器与独立服务器

（1）域控制器：域控制器是运行活动目录的 Windows Server 2003 服务器。在域控制器上，活动目录存储了所有的域范围内的账户和策略信息，如系统的安全策略、用户身份验证数据和目录搜索等。正是由于有活动目录的存在，因此域控制器不需要本地安全账户管理器（SAM）。

一个域可以有一个或多个域控制器。通常单个局域网的用户可能只需要一个域就能满足要求。由于一个域比较简单，所以整个域只需要一个域控制器。为了获得高可用性和较强的容错能力，具有多个网络位置的大型网络或组织可能在每个部分都需要一个或多个域控制器。

（2）成员服务器：一个成员服务器是一台运行 Windows Server 2003 的域成员服务器，由于不是域控制器，因此成员服务器不执行用户身份验证，并且不存储安全策略信息。这样可以让成员服务器以更高的处理能力来处理网络中的其他服务。所以，在网络中通常使用成员服务器作为专用的文件服务器、应用服务器、数据库服务器或者 Web 服务器，专门用于为网络中的用户提供一种或几种服务。

（3）独立服务器：独立服务器既不是域控制器，也不是某个域的成员，也就是说它是一台具有独立安全边界的计算机，它维护本机独立的用户账户信息，服务于本机的身份验证。独立服务器以工作组的形式与其他计算机组建成对等网。

6．用户访问资源的过程

（1）访问本地域中的资源。当用户在某一计算机登录域时，域控制器必须验证用户的身份。用户输入账户名和密码，被域控制器确认后，域控制器会替用户建立一个“访问令牌（Access Token）”，这个访问令牌包含用户的 SID、用户隶属的所有组的 SID 等数据。用户取得这个访问令牌后，在他要访问计算机的资源时（例如文件夹），出示该令牌。

如图 5.9 所示，工作站、域控制器和服务器均在 xpc.edu.cn 域中，其流程如下：

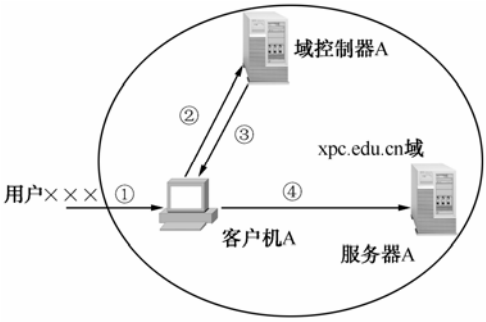

图 5.9　访问本地域中的资源

① 当用户×××从客户机 A 登录到域 xpc.edu.cn 时，首先输入账户名和密码；

② 客户机 A 向所属域内扮演 KDC 角色的域控制器 A 索取一个用来与服务器 A 沟通的服务票据；

③ 域控制器 A 检查其数据库后，发放服务票据给客户机 A；

④ 客户机 A 取得服务票据后，会将服务票据发送给服务器 A，服务器 A 读取服务票据内的用户身份数据后，会根据这些数据决定用户可以访问的资源。

（2）访问跨域的资源。如图 5.10 所示，根域 edu.cn 下有两个子域 xpc.edu.cn 和 xttc.edu.cn。×××是 xpc.edu.cn 的用户，而服务器 B 位于 xttc.edu.cn 域中，×××要访问服务器 B 上的资源，×××的计算机必须取得用来与服务器 B 沟通的服务票据，其流程如下：

① 用户×××在客户机 A 登录，输入账户名和密码；

② 客户机 A 向其所属的域控制器 A 索取一个用来与服务器 B 沟通的服务票据；

③ 域控制器 A 检查活动目录后发现服务器 B 不在自己的域内（xpc.edu.cn），就转向全局编录，询问服务器 B 位于哪一个域；

④ 全局编录根据数据库内的数据，告知域控制器 A 服务器 B 位于 xttc.edu.cn 域中；

⑤ 域控制器 A 根据信任路径，通知客户机 A 向 edu.cn 的域控制器进行查询；

⑥ 客户机 A 向 edu.cn 的域控制器查询 xttc.edu.cn 的域控制器；

⑦ edu.cn 的域控制器通知客户机 A 向 xttc.edu.cn 的域控制器 B 进行查询；

⑧ 客户机 A 向 xttc.edu.cn 的域控制器 B 索取一个能够与服务器 B 进行沟通的服务票据；

⑨ 域控制器 B 发放服务票据给客户机 A；

⑩ 客户机 A 取得服务票据后，将服务票据传给服务器 B，服务器 B 将根据服务票据授予用户×××访问资源的权利。

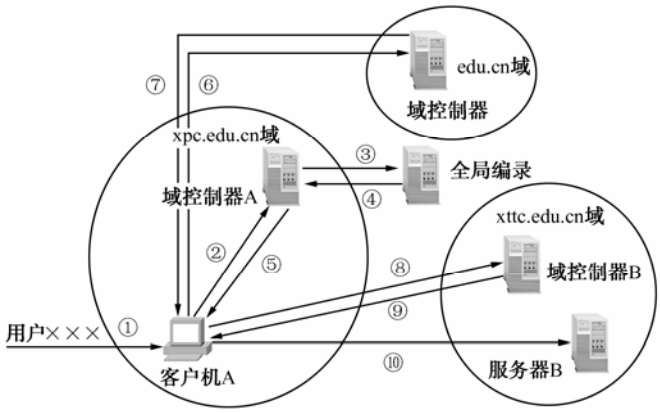

图 5.10　访问跨域资源

5.3 方案设计及准备

1．设计

有两个域树：edu.cn 和 gov.cn。其中 edu.cn 域树下有 xpc.edu.cn 子域，在 edu.cn 域中有两个域控制器；在 xpc.edu.cn 域中有一个域控制器和一个成员服务器。要求先创建 edu.cn 的域树，然后再创建 gov.cn 的域树。根据以上要求，本项目实施的网络拓扑图如图 5.11 所示。

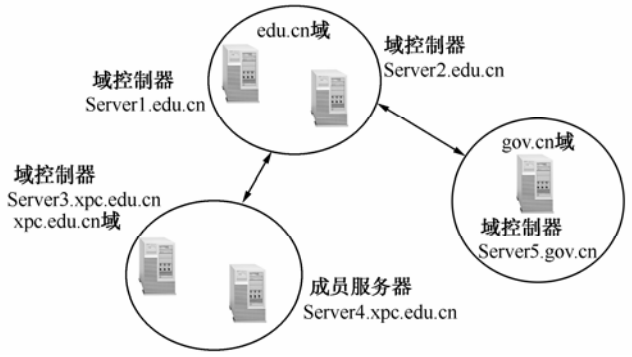

图 5.11　创建域图

2．设备清单

为了搭建图 5.11 所示的网络环境，需要如下设备：

① 安装 Windows Server 2003 的 PC 计算机 5 台；

② Windows XP 计算机 1 台；

③ Windows Server 2003 安装光盘。

5.4 项目实施

步骤 1：创建第一个域edu.cn

创建域可以把一台已经安装 Windows Server 2003 的独立服务器升级为域控制器。一般情况下，在域中如果没有 DNS 服务器存在，可以在创建域时把 DNS 一起安装上。在这里把域 edu.cn 中的 Server1 升级为域林中的第一台域控制器。步骤如下：

（1）首先确认“本地连接”属性 TCP/IP 中首选 DNS 指向了自己（假设 IP 地址为 192.168.1.100）执行“开始→管理工具→配置您的服务器向导”选项，弹出“配置您的服务器向导”对话框。

（2）单击“下一步”按钮，再次单击“下一步”按钮，弹出“服务器角色”对话框，如图 5.12 所示。选择“域控制器（Active Directory）”，单击“下一步”按钮，弹出“选择总结”对话框，单击“下一步”按钮，启动 Active Directory 安装向导。

（3）单击“下一步”按钮，弹出“操作系统兼容性”对话框，单击“下一步”按钮，弹出“域控制器类型”对话框，如图 5.13 所示。服务器若是新域中的第一个域控制器，则应选择“新域的域控制器”；如果域中已经有域控制器了，此域控制器只是作为域的额外控制器，则可以选择“现有域的额外域控制器”。

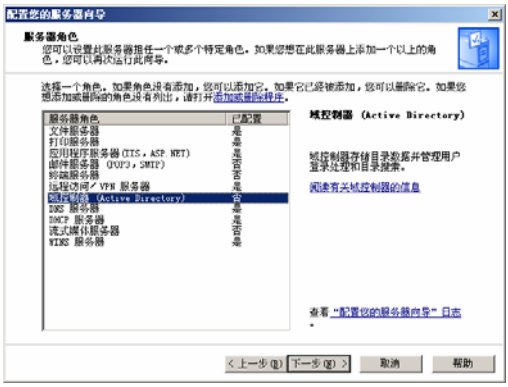

图 5.12 “服务器角色”对话框

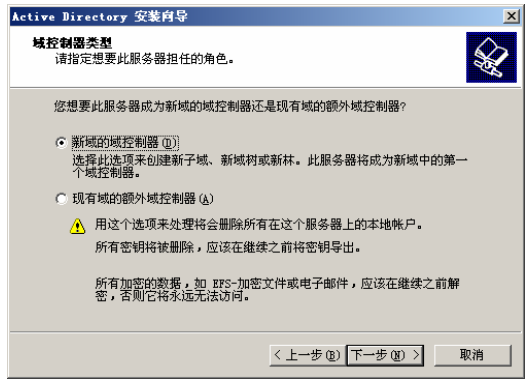

图 5.13 “域控制器类型”对话框

（4）单击“下一步”按钮，弹出“创建一个新域”对话框，如图 5.14 所示。如果是整个组织中的第一个域或者想让该域完全独立于原有的林，则选择“在新林中的域（默认）”；若想让该域成为原来的域中的子域，则应选择“在现有域树中的子域”；若不想让该域成为现有域的子域，则选择“在现有的林中的域树”。

（5）单击“下一步”按钮，弹出“新的域名”对话框，如图 5.15 所示。在“新域的 DNS 全名”中输入 edu.cn。

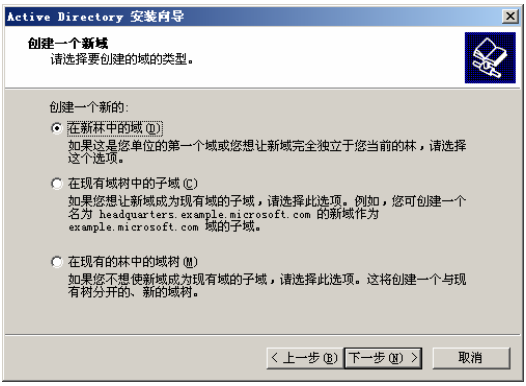

图 5.14 “创建一个新域”对话框

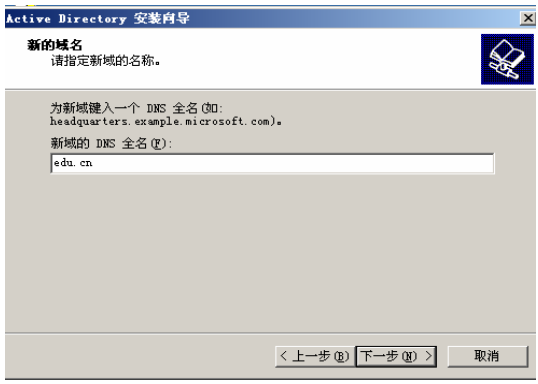

图 5.15 “新的域名”对话框

（6）单击“下一步”按钮，弹出“NetBIOS 域名”对话框，如图 5.16 所示，默认接受将 EDU 作为默认“域 NetBIOS 名”。

图 5.16 “NetBIOS 域名”对话框

图 5.17 “数据库和日志文件文件夹”对话框

（7）单击“下一步”按钮，弹出“数据库和日志文件文件夹”对话框，如图 5.17 所示，接受默认设置。

（8）单击“下一步”按钮，弹出“共享的系统卷”对话框，如图 5.18 所示，接受默认设置。

（9）单击“下一步”按钮，弹出“DNS 注册诊断”对话框，如图 5.19 所示。选择“在这台计算机上安装并配置 DNS 服务器，并将这台 DNS 服务器设为这台计算机的首选 DNS 服务器”单选项。

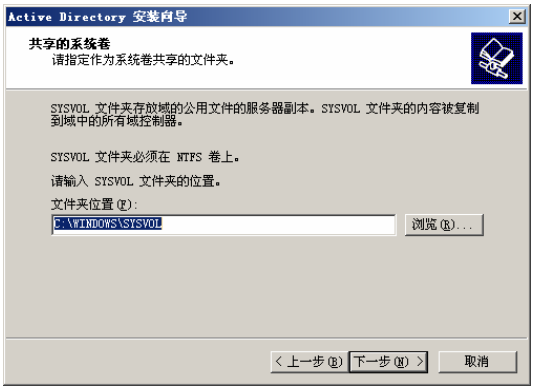

图 5.18　“共享的系统卷”对话框

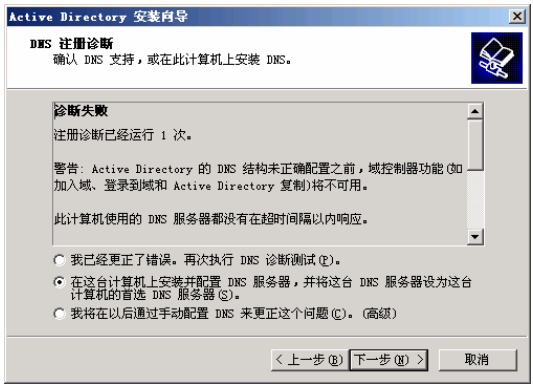

图 5.19　“DNS 注册诊断”对话框

（10）单击“下一步”按钮，弹出“权限”对话框，接受默认设置。

（11）单击“下一步”按钮，弹出“目录服务还原模式的管理员密码”对话框，如图 5.20 所示，在“还原模式密码”和“确认密码”栏输入相同的密码。

（12）单击“下一步”按钮，弹出“摘要”对话框，如图 5.21 所示，显示安装的一些基本信息摘要。

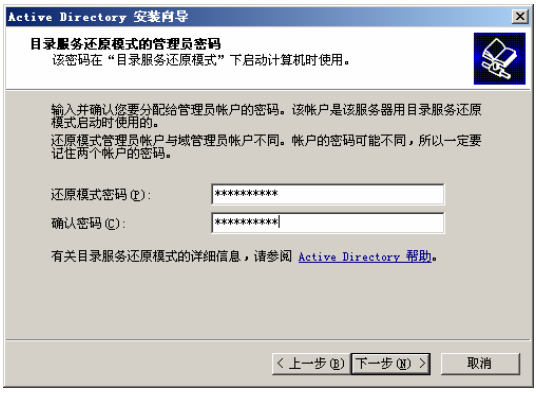

图 5.20　目录服务还原模式的管理员密码

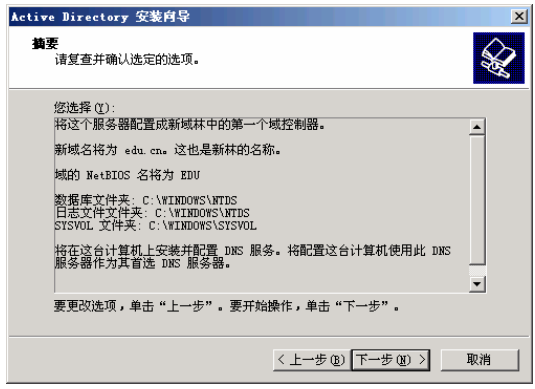

图 5.21　“摘要”对话框

（13）单击“下一步”按钮，开始安装 Active Directory。在出现提示时，要插入 Windows Server 2003 安装光盘。

（14）单击“完成”按钮，重新启动计算机。

也可以在“运行”栏中，输入“dcpromo”，然后单击“确定”按钮，以下安装步骤同上。

步骤 2：添加额外的域控制器

在一个安装 Windows Server 2003 系统的组成域中可以有多个地位平等的域控制器，它们

都有所属域的活动目录的副本，多个域控制器可以分担用户登录时的验证任务，同时还能防止单一域控制器的失败所导致网络的瘫痪。在域中的某一个域控制器上添加用户时，域控制器会把活动目录的变化复制到域中别的域控制器上。在域中安装额外的域控制器，需要把活动目录从原有的域控制器复制到新的服务器上。下面以图 5.11 中的 Server2 服务器为例来说明添加额外域控制器的过程。

（1）设置 TCP/IP 协议，保证 Server2 服务器和 Server1 服务器能够通信，并且配置 TCP/IP 协议的首选 DNS 指向 Server1。

（2）在“运行”对话框中输入“dcpromo”，启动活动目录安装向导；在欢迎对话框和操作系统兼容性说明对话框中，直接单击“下一步”按钮，弹出“域控制器类型”对话框。如图 5.13 所示。选择“现有域的额外域控制器”单选按钮。

（3）单击“下一步”按钮，弹出“网络凭据”对话框，如图 5.22 所示。输入原有域的域名、管理员账户和密码。

（4）单击“下一步”按钮。安装向导和原有的域控制器进行联系验证信息，弹出“额外的域控制器”对话框，如图 5.23 所示，要求输入原有域的 DNS 名称，如 edu.cn，单击“下一步”按钮，输入活动目录数据库文件和日志文件夹的位置。

图 5.22 “网络凭据”对话框

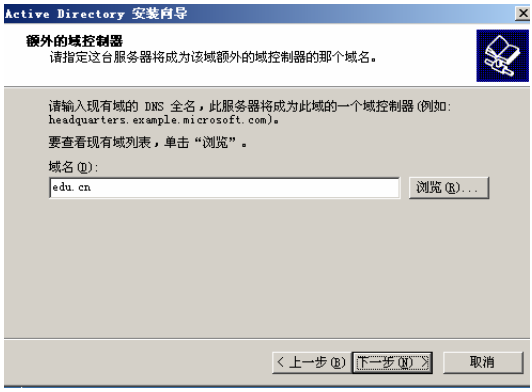

图 5.23 “额外的域控制器”对话框

（5）单击“下一步”按钮，随后的步骤和创建域林中的第一个域控制器时的步骤一样，在这里不再详述。最后单击“确定”按钮后，安装向导从原有的域控制器上开始复制活动目录。完成安装后，重新启动计算机。

（6）用管理员身份登录，在“开始→管理工具→Active Directory 用户和计算机”窗口中，可以看到 edu.cn 有两个域控制器，如图 5.24 所示。

步骤 3：创建子域

同样，创建子域要先安装一台独立服务器，然后将这台服务器提升为子域的域控制器。下面以图 5.13 中建立 xpc.edu.cn 子域为例来说明创建步骤。

（1）设置 TCP/IP 协议保证 Server3 服务器和 Server1 服务器能够通信，并且配置 TCP/IP 协议的首选 DNS 指向用来支持父域 edu.cn 的 DNS 服务器 Server1。

（2）在“运行”对话框中输入 dcpromo，启动活动目录安装向导；在欢迎对话框和操作系统兼容性说明对话框中，直接单击“下一步”按钮，弹出“域控制器类型”对话框。如图 5.13 所示。选择“新域的域控制器”单选按钮。

（3）单击“下一步”按钮，弹出“创建一个新域”对话框，如图 5.14 所示。选择“在现有域树中的子域”单选按钮。

（4）单击“下一步”按钮，弹出“网络凭据”对话框，如图 5.22 所示，输入原有域的域名、管理员账户和密码。

（5）单击“下一步”按钮，弹出“子域安装”对话框，如图 5.25 所示。输入父域的域名和新的子域的域名（子域的域名不需要包括父域的域名）。

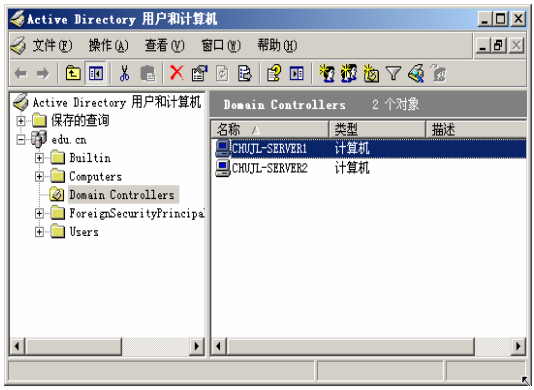

图 5.24　Active Directory 用户和计算机

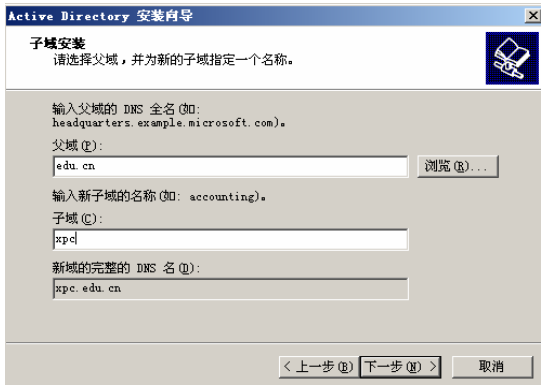

图 5.25　“子域安装”对话框

（6）单击“下一步”按钮，弹出“NetBIOS 域名”对话框，如图 5.26 所示，输入子域的 NetBIOS 名，单击“下一步”按钮。

（7）随后的步骤和创建域林中的第一个域控制器时的步骤一样，在这里不再详述。依次单击“确定”按钮后，安装向导开始安装活动目录，通常需要几分钟才能完成。完成安装后，重新启动计算机。

（8）用管理员身份登录，在“开始→管理工具→Active Directory 用户和计算机”窗口中，可以看到 edu.cn 下有 xpc.edu.cn 子域了。

图 5.26　NetBIOS 域名

步骤 4：创建域林中的第二棵域树

仍然以图 5.13 中的 Server1 作为 Server5 的 DNS 服务器为例来介绍。

（1）设置 TCP/IP 协议保证 Server5 服务器和 Server1 服务器能够通信，并且配置 TCP/IP 协议的首选 DNS 指向了 DNS 服务器 Server1。

（2）在“运行”对话框中输入 dcpromo 命令，启动活动目录安装向导；在欢迎对话框和操作系统兼容性说明对话框中，直接单击“下一步”按钮，弹出“域控制器类型”对话框。选择“新域的域控制器”单选按钮。

（3）单击“下一步”按钮，弹出“创建一个新域”对话框。选择“在现有的林中的域树”单选按钮。

（4）单击“下一步”按钮，弹出“网络凭据”对话框，输入原有域的域名、管理员账户和密码。

（5）单击“下一步”按钮，弹出“新域目录树”对话框，如图 5.27 所示。输入新域树根

域的 DNS 名，这里应为 gov.cn。

（6）单击“下一步”按钮，弹出“NetBIOS 域名”对话框，如图 5.28 所示，输入新域的 NetBIOS 名，默认为 GOV。

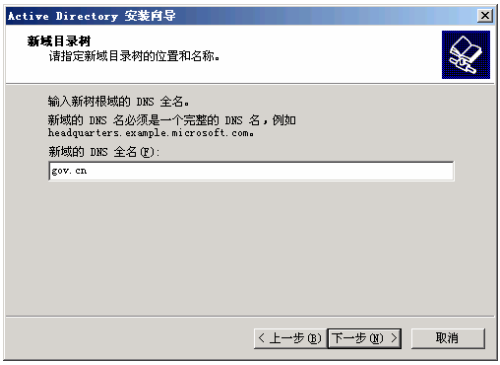

图 5.27 “新域目录树”对话框

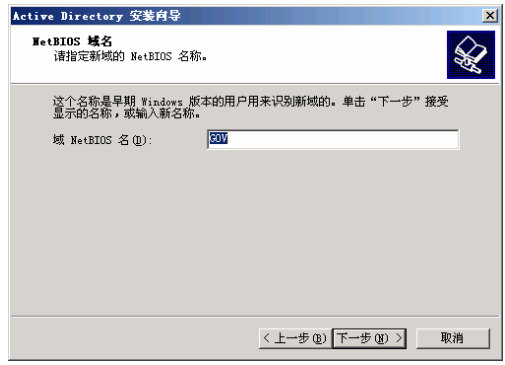

图 5.28 “NetBIOS 域名”对话框

（7）单击“下一步”按钮，随后的步骤和创建域林中的第一个域控制器时的步骤一样，在这里不再详述。依次单击“确定”按钮后，安装向导开始安装活动目录，通常需要几分钟才能完成。完成安装后，重新启动计算机。

（8）用管理员身份登录，打开“开始→管理工具→Active Directory 域和信任关系”窗口，可以看到 gov.cn 域已经存在了。

步骤 5：域控制器降级为成员服务器

Windows Server 2003 服务器在域中可以有 3 种角色：域控制器、成员服务器和独立服务器。

当一台 Windows Server 2003 成员服务器安装了活动目录后，服务器就成为域控制器，域控制器可以对用户的登录等进行验证；然而 Windows Server 2003 成员服务器可以仅仅加入到域中，而不安装活动目录，这时服务器的主要目的是为了提供网络资源，这样的服务器称为成员服务器。严格说来，独立服务器和域没有什么关系，如果服务器不加入域中也不安装活动目录，服务器就称为独立服务器。服务器的这三种角色可以发生改变，如图 5.29 所示。

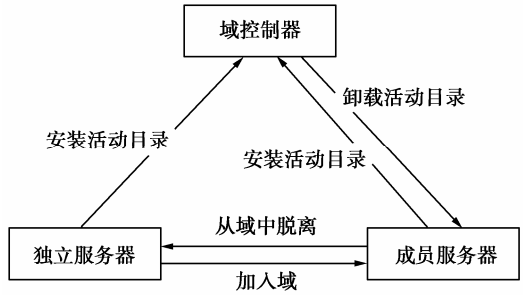

图 5.29 服务器角色的转换

在域控制器上把活动目录删除，域控制器就降为成员服务器了。下面以图 5.13 中的 Server2.edu.cn 降级为例来介绍其步骤。

（1）在“运行”栏中输入“dcpromo”命令，单击“确定”按钮，启动 Active Directory

安装向导，单击“下一步”按钮，弹出“删除 Active Directory”对话框，如图 5.30 所示。

（2）如果该服务器是域中的最后一个域控制器，选中“这个服务器是域中的最后一个域控制器”复选框，此处，edu.cn 还有另外一个域控制器 Server1.edu.cn 存在。单击“下一步”按钮，弹出“管理员密码”对话框，输入活动目录服务还原模式的管理员密码。

（3）单击“下一步”按钮，确认从服务器上删除活动目录后，服务器就成为 edu.cn 域上的一台成员服务器，单击“确定”按钮后，安装向导从该计算机删除活动目录。

（4）删除完毕后，重新启动计算机，这样就把域控制器降为成员服务器。

图 5.30 “删除 Active Directory”对话框

步骤 6：独立服务器升级为成员服务器

下面以图 5.14 中的 Server4 服务器加入到 xpc.edu.cn 域为例说明独立服务器升级为成员服务器的步骤。

图 5.31 “计算计名称更改”对话框

（1）设置 Server4 服务器上 TCP/IP 协议的首选 DNS 指向了 DNS 服务器 Server1。

（2）选择“开始→控制面板→系统”菜单，弹出“系统属性”对话框，选择“计算机名”标签，单击“更改”按钮，弹出“计算机名称更改”对话框，如图 5.31 所示。

（3）在“隶属于”选项区域中，选择“域”单选按钮，并输入要加入的域的名字 xpc.edu.cn，单击“确定”按钮，弹出“计算机名称更改”对话框，输入要加入的域的管理员账户和密码，单击“确定”按钮后，重新启动计算机即可。

步骤 7：成员服务器降级为独立服务器

选择“开始→控制面板→系统”菜单，弹出“系统属性”对话框，选择“计算机名”标签，单击“更改”按钮，弹出“计算机名称更改”对话框，在“隶属于”选项区域中，选择“工作组”单选按钮，并输入从域中脱离后要加入的工作组的名字，单击“确定”按钮，弹出“计算机名更改”对话框，输入要脱离的域的管理员账户和密码。单击“确定”按钮后，重新启动计算机即可。

步骤 8：Active Directory用户和计算机的管理

Active Directory 用户和计算机的管理主要包括以下几点。

（1）选择“开始→管理工具→Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，如图 5.32 所示。

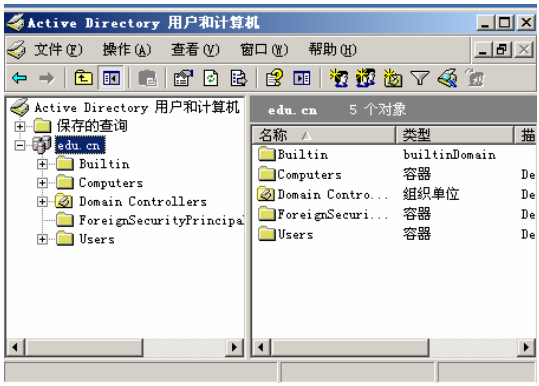

图 5.32 “Active Directory 用户和计算机”窗口

（2）在“Active Directory 用户和计算机”窗口的左部，选中“Computers”选项，可以显示当前域中的计算机，即成员服务器和客户机。

（3）在“Active Directory 用户和计算机”窗口的左部，选中“Domains Controllers”选项，可以显示当前域中的域控制器。

（4）在“Active Directory 用户和计算机”窗口的左部，选中“Users”或“Builtin”选项，可以显示当前域中的用户或组等情况。

（5）组织单元可以用来逻辑地组织用户、组、计算机等，反映了企业行政管理的实际框架。创建组织单元的步骤为：在“Active Directory 用户和计算机”窗口左部的域树中选中edu.cn，右击鼠标，执行“新建→组织单元”命令，弹出“新建对象-组织单元”对话框，输入组织单元名称，单击“确定”按钮即可。

步骤 9：将计算机加入到域中

局域网中的计算机必须先加入到域中，在域控制器上注册计算机账户后，用户才能使用该计算机登录到域中。

要将网络中的计算机加入到域中，有两种操作方法。第一种方法是具有域管理员权限的网络管理人员亲自到客户计算机上操作，其操作步骤如下：

（1）管理人员打开要加入域的计算机，并且以本地计算机管理员的身份登录，然后在计算机的 IP 设置中，将 DNS 服务器指向能够解析域名的 DNS 服务器，本例中为域控制器。

（2）在“我的电脑”上单击鼠标右键，选择“属性”命令，打开“系统属性”对话框。

（3）选择“计算机名”选项卡，如图 5.33 所示，单击“更改”按钮，打开“计算机名称更改”对话框，选择加入到“域”，并输入新的计算机名和要加入的域名，单击“确定”按钮。

（4）此时计算机将寻找网络中的域控制器，然后打开“计算机名称更改”对话框，如图 5.34 所示，输入域管理员的用户名和密码。因为默认只有域管理员才能将计算机加入到域中。

（5）在域控制器验证通过后，就将该计算机加入到域中，弹出欢迎加入域的对话框，然后重新启动计算机，就可以在此计算机登录进入域了。

在域控制器的“Active Directory 用户和计算机”管理工具中，选择“计算机”，可以看到已经为刚才的客户计算机自动建立了一个计算机账户。

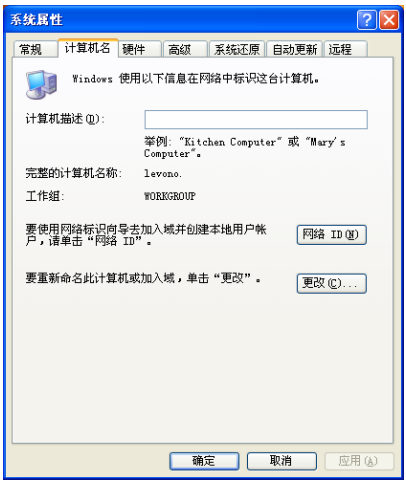

图 5.33 “系统属性”对话框

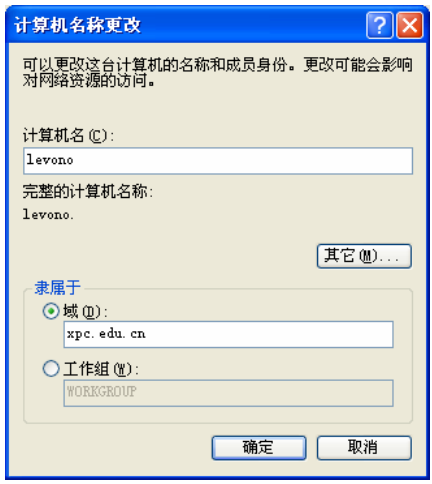

图 5.34 “计算机名称更改”对话框

习 题

一、名词解释

1．域　　2．活动目录　　3．域控制器　　4．成员服务器　　5．独立服务器

二、填空题

1．域采用集中式的管理方式，域中所有用户身份验证，权限管理等操作都是在_____上完成的，它是整个域的核心，简写为 DC。

2．可以将一台普通的 Windows Server 2003 服务器升级为域控制器的命令是_____。

3．域树中的子域和父域的信任关系是_____、_____。

4．活动目录存放在_____中。

5．Windows Server 2003 服务器的三种角色是_____、_____、_____。

6．独立服务器上安装了_____就可升级为域控制器。

三、选择题

1．通过下面哪种方法可以在服务器上安装活动目录？（　　）

A．管理工具/配置服务器

B．管理工具/计算机管理

C．管理工具/Internet 服务管理器

D．以上都不是

2．安装域控制器时，活动目录必须安装到（　　）分区上。

A．FAT　　B．FAT32　　C．NTFS　　D．SWAP

3．要想在域树中填加一个子域，必须是具有（　　）管理员权限的用户才可以完成。

A．该子域的父域管理员　　B．当前子域管理员

C．企业管理元组　　D．活动目录管理员

4．域树中的域通过（　　）关系连接在一起，相互之间可以访问。

A．父子　　B．信任　　C．层次　　D．树形

四、简答题

1．什么是 Windows Server 2003 活动目录？它有什么特点？

2．什么是域控制器？什么是成员服务器？两者之间有什么关系？

3．在工作组中，用户账户存放在什么位置？

4．在域模式中，用户账户存放在什么位置？

5．什么时候需要多个域树？

6．活动目录中存放了什么信息？

五、实训题

在域中新建一个域用户 student，新建一个全局组 xxgcx，把 student 加入到全局组 xxgcx 中，并设置域用户只能在 8:30～11:30 登录。

项目 6　域用户账户、组的管理

6.1　项目内容

1．项目目的

通过在域模式下对 Windows Server 2003 服务器进行配置和管理，掌握中小型网络环境中对用户、组的管理，以及安全管理，理解工作组模式和域模式的区别，理解域模式的概念，掌握域模式的应用和管理。

2．项目任务

某公司组建了单位内部的基于域模式的局域网，其中有一台域控制器，有一台文件服务器兼打印服务器的计算机，以及数百台桌面计算机，域控制器管理着公司里众多的用户，现在需要合理地配置文件服务器，使每位员工都能将各自的文件备份到文件服务器上，同时配置打印服务器，对公司的打印机进行有效地管理。

3．任务目标

① 学会规划域服务器中的工作组；
② 学会在域服务器中创建和管理组；
③ 学会在域服务器中添加和管理域用户账户；
④ 学会在域服务器中规划和设置域用户账户的权限。

6.2　相关知识

6.2.1　域用户账户

Active Directory 用户账户和计算机账户代表物理实体，如人或计算机。用户或计算机账户用于：

① 验证用户或计算机的身份；
② 授权或拒绝访问域资源；
③ 管理其他安全实体；
④ 审核使用用户或计算机账户执行的操作。

6.2.2　域用户组

Active Directory 中的组是驻留在域和组织单位容器对象中的目录对象。Active Directory 在安装时提供了一系列默认的组，它也允许后期根据实际需要创建组。域用户组是在域控制器上建立的，其信息存储在 Active Directory 数据库中，这些用户组能够被使用在整个域中的计算机上。

1．组类型

根据域用户组的权限，Active Directory 中有以下两种组类型：

① 通信组：仅用于电子邮件分发列表或简单的管理分组。无法设置该组的权限。

② 安全组：可用于定义对资源和对象的访问权限，也可以作为电子邮件实体。

2．组的作用域

与工作组模式下的组有较大区别，域模式下的组都有一个作用域，用来确定在域树或林中该组的应用范围。Active Directory 域组有三类不同的组作用域：全局组、本地域组和通用组。

（1）全局组。全局组主要用来组织用户，可以将多个权限相似的用户账户加入到同一全局组内。全局组的特点如下：

① 全局组内的成员，只能够包含该组所属的域内的用户账号与全局组，也就是说，只能够将同一域内的用户账户与其他全局组加入到全局组内；

② 全局组可以访问任何一个域内的资源，也就是说，可以在任何一个域内设置某个全局组的使用权限，以便让此全局组具备权限来访问该域内的资源。

（2）本地域组。本地域组主要用来指派其在所属域内的访问权限，以便可以访问该域内的资源。本地域组的特点如下：

① 本地域组内的成员，能够包含任何一个域内的用户账号、通用组、全局组，也能够包含同一域内的本地域组，但是无法包含其他域内的本地域组；

② 本地域组只能够访问同一域内的资源，无法访问其他域内的资源。换句话说，在设置本地域组的权限时，只可以设置同一域内的资源的权限，但是无法设置其他域内的资源的权限。

（3）通用组。通用组主要用来指派在所属域内的访问权限，以便可以访问每一域内的资源。通用组的特点如下：

① 通用组内的成员，能够包含任何一个域内的用户账号、通用组、全局组，但是它无法包含任何一个域内的本地域组；

② 通用组可以访问任何一个域内的资源，也就是说，可以在一个域内设置通用组的权限，以便让此通用组具备权限来访问该域内的资源。

在单一域的网络环境下，利用组来管理网络资源时，为了便于管理，建议采用以下的准则。

- 建立一个全局组，然后将具备相同权限的用户账户加入到该组内。例如，将计算机教研室所有教师的用户账号加入到一个称为“jsjjys”的全局组内。
- 建立一个本地域组，设置此组对某些资源具备适当的权限。例如，有一个激光打印机供某些用户来打印，建立一个称为“LJP”的本地域组。
- 将所有需要该资源访问权限的全局组加入到本地域组内。例如，将“jsjjys”全局组加入到“LJP”本地域组内。
- 指定适当的权限给本地域组。例如，给“LJP”本地域组对此激光打印机的使用权限。

也就是将用户账号加入到全局组内，再将此全局组加入到本地域组内，最后指派适当的权限给本地域组。经过这些步骤后，上述用户账号就会具备相应的权限。

3．内置的域组

在安装完 Windows Server 2003 后，系统会建立一些用户组。通常这些组是为区分系统管理工作的权限所设立的，不同的组有不同的资源存取权限。在 Windows Server 2003 中拥有多种类别的内置域组。

1）本地域组（Domain Local Group）

- Account Operators（账户操作员）：该组的成员具有操作使用者管理员所属域的账户与组，并可设置账户的进阶权限。但是该组成员无法修改 Administrator 与任何的 Operators 组。
- Administrator：该组的成员可以完全不受限制地存取计算机域的资源，可以说是最具有权力的组。在预设的情况下，Administrator 账户与 Domain Admins 全局组都是该组的成员。
- Backup Operators：该组的成员可使用 Windows 备份工具来进行备份和还原的工作，但只能因为备份或还原文件才能覆盖安全性限制。
- Guests：该组的成员只能享有管理员授予的权限，以及存取指定权限的资源。在预设的情况下，Guests 账户与 Domain Guests 全局组都是该组的成员。
- Printer Operators：该组的成员可以管理域打印机，包括建立、管理及删除网络打印机。
- Replicator：该组的成员支持域中的文件复制，可启动目录复制程序进行目录复制。
- Server Operator：该组的成员可以管理域服务器，包括建立、管理及删除任何服务器的共用目录、管理网络打印机、备份任何服务器的文件、格式化服务器硬盘、锁定服务器及变更服务器的系统时间等权限。
- Users：该组的成员会被防止制造意外或有意的全面系统变更。因此他们只可以执行得到授权的应用程序，不可执行大部分的继承应用程序。

2）全局组（Global Group）

- Domain Admins：该组可以代表具有操作域权力的用户，在预设的情况下，Domain Admins 会隶属于 Administrator 本地域组，因此该组的成员可以在域中执行管理工作。Windows Server 2003 不会将任何建立的账户放到 Domain Admins 组中，而内建的 Administrator 账户是其唯一的成员。因此，如果希望某一用户成为域系统管理员，建议将该用户账户加至 Domain Admins 组中，而不要直接加至 Administrator 组。
- Domain Guests：代表所有域来宾的组，Windows Server 2000 会自动将用户使用的账户加至该组，并将该组加至内建本地域 Guests 组中。
- Domain Users：代表所有域成员的组，在预设的情况下，任何建立的用户账户都会是 Domain Users 组的成员；而任何所建立的计算机账户都会是 Domain Computers 组的成员。如果希望让所有的账户都具有某种资源的存取权限，则可以将该权限指定给 Domain Users 组或让 Domain Users 组属于具有该权限的组。Domain Users 组在预设的情况下是内建本地域 Users 组的成员。
- Enterprise Admins：Windows Server 2003 提供了授权具有管理整个网络权力用户的方法，该方法就是将用户账户加至 Enterprise Admins 组，然后再将该组加至每个域的 Administrator 本地域组内。

3）本地组（Local Group）

当将 Windows Server 2003 安装成独立服务器或成员服务器时，他们都拥有内建的本地

组。内建的本地组提供了在单一的计算机上执行系统工作的权力。

- Administrators：该组的成员可以完全不受限制地存取本地计算机的资源，而内建的 Administrator 用户账号为该组的预设成员。在该计算机加入一个域之后，域上的 Domain Admins 会自动被加入该计算机的 Administrators 组之中，这表示域上具有系统管理员身份的用户在本地也具有系统管理员的身份。
- Backup Operators：该组的成员可以使用 Windows 备份工具来进行备份和还原的工作，但只能因为备份或还原文件才能覆盖安全性限制。
- Guests：该组的成员只能享有管理员授予的权限，以及存取指定权限的资源。在预设的情况下，Guest 账户与 Domain Guests 全局组都是该组的成员。在该计算机加入一个域之后，域上的 Domain Guests 组会自动被加入计算机的 Guests 组之中。
- Power users：该组的成员可以新建、删除、修改本地用户账户，并且拥有管理本地共享文件夹与打印机的权力。
- Replicator：该组的成员支持域中的文件复制，可启动目录复制程序进行目录复制。
- Users：该组的成员会被防止制造意外的全面系统变更，因为他们只可以得到授权的应用程序，不可执行大部分的继承应用程序。在该计算机加入一个域之后，域上的 Domain Users 会自动被加入该计算机的 Users 之中。

4）系统组（System Group）

- Everyone：指所有访问这台计算机的用户，因此在指定权限时需要特别小心，尤其是启用 Guest 账户时。原因是未经授权的用户可以通过 Guest 连上域，而 Guest 也是 Everyone 组的成员。
- Authenticated Users：经过授权的合法用户，为了防止上述在 Everyone 组中所描述的问题，可以通过 Authenticated Users 权限的指定来代替 Everyone 组的权限的指定，以防止匿名用户存取不当资源。
- Interactive：任何在本地登录的用户。
- Network：通过网络连接到本地的用户。
- Anonymous Logon：匿名进入（未经合法授权）的用户。
- Dialup：拨号连接的用户。

6.3 方案设计及准备

1．设计

为了完成项目任务，设计一个小型网络，拥有 3 台计算机，这 3 台计算机组成一个基于工作组的小型网络，现在需要对这些计算机进行配置，以满足下列要求：

（1）公司内有 5 位员工，需要使用这些计算机，每位用户的部门、用户账户初始密码等信息见表 6.1。

表 6.1　用户账户

部门	用户账户名称	用户全名	描述	初始密码
总经理	Zongjl	张三	总经理	Zongjl
财务部	Caiwbjl	王五	财务部经理	Caiwbjl
财务部	Caiwbyg1	马六	财务部员工	Caiwbyg1
销售部	Xiaosjl	李四	销售部经理	Xiaosbjl
销售部	Xiaosbyg1	赵七	销售部员工	Xiaosbyg1

（2）为方便管理，将上述用户组织为具有不同权限的组，见表 6.2。

表 6.2　共享资源的权限分配

组名	描述	组类型	作用域	成员
GenaralMgr	总经理	安全组	全局	张三
Managers	各部门经理	安全组	全局	李四、王五
Financial	财务部	安全组	全局	王五、马六
Sales	销售部	安全组	全局	李四、赵七
Staff	全体员工	安全组	全局	全体员工用户
Colorprinter	彩色打印	安全组	本地域组	GenaralMgr、Managers
Printerhigh	高优先级打印	安全组	本地域组	GenaralMgr
Printerlow	低优先级打印	安全组	本地域组	Staff

① 所有用户在文件服务器上都有一个私有文件夹，用户本人有完全控制权限，其他用户有读权限。

② 打印服务器上安装了两台打印机，一台是彩色激光打印机，打印成本高，供总经理及各部门经理使用，另一台是普通激光打印机，供公司所有员工使用。公司内打印量很大，总经理在普通激光打印机的打印作业应该优先得到满足。

③ 全体员工只有在上班时间才能使用计算机。

（3）本项目实施的网络拓扑结构如图 6.1 所示。

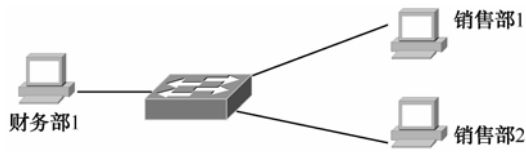

图 6.1　网络拓扑图

2．设备清单

为了搭建图 6.1 所示的网络环境，需要如下设备：

① PC 计算机 3 台，安装有 Windows Server 2003 操作系统，作为独立服务器，每台计算机的磁盘中有 NTFS 和 FAT32 文件系统的分区；

② 交换机 1 台；

③ 直通线 3 条。

6.4 项目实施

步骤 1：域用户账户创建

必须使用“Active Directory 用户和计算机”管理单元来建立域用户账户。当使用这个管理单元来建立用户账户时，这个账户会被自动建立在 MMC 控制台所找到的第一台域控制器内，以后该账户会被自动复制到此域内的所有域控制器内。

在建立用户账户时，可以选择一个组织单位，以便将用户账户建立到此组织单位内。可以将账户建立在内置的 User 组织单位或其他自行建立的组织单位内。

（1）选择“开始→管理工具→Active Directory 用户和计算机”命令，弹出“Active Directory 用户和计算机”对话框，右击“user”，选择“新建→用户”命令。弹出“新建对象-用户”对话框，如图 6.2 所示，进行如下的设置：

- “姓”与“名”：至少在这两个文本框之一输入信息。
- “姓名”：用户的全名，默认为前面的姓与名两者的结合。
- “用户登录名”：这是用户用来登录域所使用的名称，在活动目录内，这个名称必须是唯一的。
- “用户登录名（Windows Server 2000 以前版本）”：这个名称是供使用 Windows Server 2000 以前版本的用户（如 Windows NT、Windows 9×等）使用的，即用户在这些计算机上登录时，必须使用这个名称。

图 6.2　新建域用户账户（用户名设置）

（2）单击“下一步”按钮，弹出如图 6.3 所示的对话框，在“密码”与“确认密码”文本框输入用户账户的密码。为了避免在输入时被他人看到密码，因此在对话框中的密码只会以星号（*）显示，需要再次输入密码来确认所输入的密码是否正确。密码最多为 128 个字符，密码的大小写是有区别的。

- 用户密码选项的配置与在本地用户中一样。

（3）单击“下一步”按钮后，提示用户账户的信息，最后单击“完成”按钮，完成用户账户的创建。

所有新创建的域用户账户，可以被用来在网络上从成员服务器登录，但无法直接在域控制器登录，除非被赋予“本地登录”的权限。

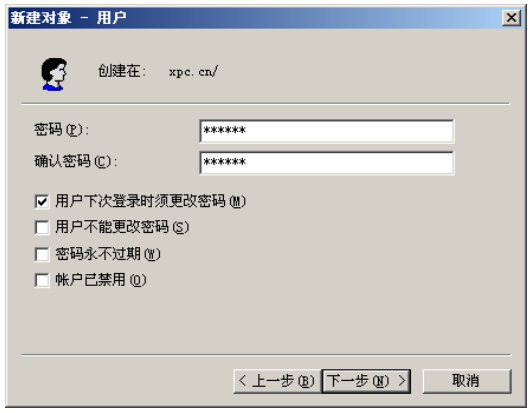

图 6.3　新建域用户账户（密码设置）

步骤 2：域用户账户的属性设置

每个域用户都有一些相关的属性可供设置，如地址、电话、传真、电子邮件、账户有效期限等。将用户的这些信息输入完毕后，就可以通过这些信息来查找活动目录内的用户。

设置用户账户的属性时，右击该用户，选择“属性”选项，打开“域用户账户属性”对话框。

1）用户个人信息的设置

所谓“用户个人信息”，就是指姓名、地址、电话、传真、移动电话、公司、部门、职称、电子邮件、网页等。

- 常规：用来设置姓、名、显示名称、描述、办公室、电话号码、电子邮件和网页等信息，如图 6.4 所示。
- 地址：用来设置国家（地区）、省/自治区、县市、街道、邮政信箱和邮政编码等信息。
- 电话：用来设置家庭电话、移动电话、传真、IP 电话等信息。
- 单位：用来设置职务、部门、公司、经理和直接下属等信息。

2）账户信息的设置

选择“账户”选项卡，如图 6.5 所示。在这里介绍用户账户的“账户过期”、“登录时间”及“登录到”的设置。

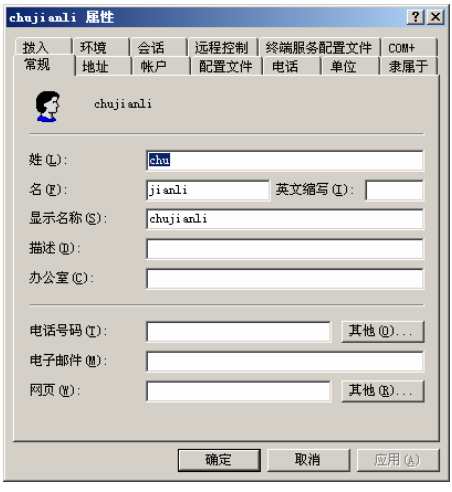

图 6.4　“常规”选项卡

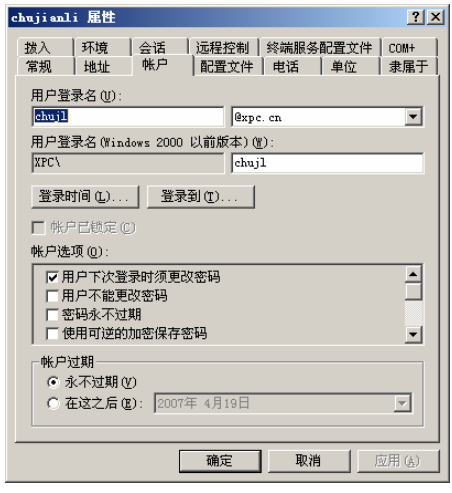

图 6.5　“账户”选项卡

（1）账户过期。设置账户的有效期限，默认为账户永不过期，也可以选择“在这之后”单选框，并确定账户过期的时间。

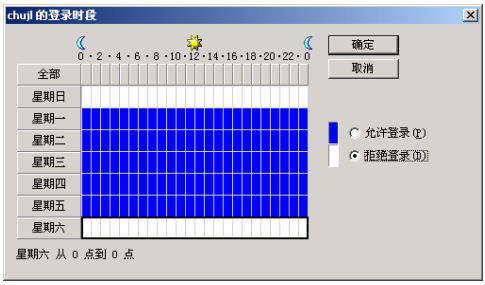

图 6.6 “登录时段”对话框

（2）登录时间。“登录时间”用来设置允许用户登录到域的时段，默认为用户可以在任何时段登录域。设置时，单击图 6.5 中的“登录时间”按钮，弹出“用户登录时段”对话框，如图 6.6 所示。在图 6.6 中，每一方块代表一小时，横轴代表一天。

选择要设置的时段，若单击“允许登录”单选按钮，表示允许用户在该时段内登录；若单击“拒绝登录”单选按钮，表示在所选的时段内，不允许用户登录。

当用户在允许使用的时段内登录连接，并且一直连接到超过允许使用的时段时，可能出现下面两种情况：

- 用户可以继续访问已经连接的资源，但是不允许再进行任何新的连接，而且用户注销后，就无法再次登录；
- 强迫中断用户的连接。

至于会发生哪一种情况，需要根据在“组策略→计算机配置→Windows 设置→安全设置→本地策略→安全选项→当登录时间用完时自动注销用户”的设置而定。

（3）登录到。“登录到”用来设置允许用户登录到域的计算机，系统默认为用户可从任何一台计算机登录域，也可以限制用户只能从某些计算机登录域。

设置时单击图 6.5 中的“登录到”按钮，弹出如图 6.7 所示的对话框，若要限制用户只能够从某台计算机登录，则选择“下列计算机”单选框，并在“计算机名”处输入此计算机的计算机名称后单击“添加”按钮，最后单击“确定”按钮完成设置。

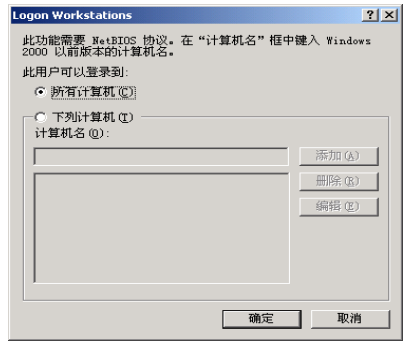

图 6.7 “设置允许登录”对话框

步骤 3：管理域用户账户

选择“开始→程序→管理工具→Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”对话框，右击用户账户，打开如图 6.8 所示的快捷菜单，然后选择相应的命令来管理域用户账户。

（1）复制：可以复制具有相同属性的账户，简化管理员的工作。

（2）停用账户/启用账户：若账户在某一时间内不使用，则可以将其停用；待需要使用时，再将其重新启用。在图 6.8 中看到的是“禁用账户”选项，如果该账户已被停用，则此处会变为“启用账户”。

（3）重命名：可以将该账户改名，由于其安全识别码（SID）并没有改变，因此其账户的属性、权限设置与组关系都不会受到影响。

（4）删除账户：可以将不再使用的账户删除，以免占用活动目录的空间。将账户删除后，即使再添加一个相同名称的账户，这个新账户也不会继承原账户的权限、权力与组关系，因为它们具有不同的 SID。

图 6.8 “管理域用户账户”对话框

（5）重设密码：当用户忘记密码或密码使用期限到期时，可以利用此命令重新为用户设置一个新的密码。

（6）解除被锁定的用户：在账户策略内可以设置用户输入密码失败多次时将该账户锁定。当用户账户被锁定时，可以在“Active Directory 用户和计算机”对话框中选定该用户并单击鼠标右键，再从弹出的快捷菜单中依次选择“属性→账户”命令，将“账户被锁定”的复选框清除即可。

步骤 4：域组的添加、删除与更名

（1）添加域组的步骤如下。

① 在“Active Directory 用户和计算机”对话框选择域名或某个组织单位，单击鼠标右键，从弹出的快捷菜单中选择“新建”→“组”命令，打开“新建对象-组”对话框，如图 6.9 所示。

② 在“组名”文本框中输入域组的名称，在“组名（Windows Server 2000 以前版本）”文本框中输入供旧操作系统访问的组名。

③ 在“组作用域”复选框中选择组的使用领域：“本地域”、“全局”或“通用”。

④ 在“组类型”复选框中选择组的类型：“安全式”或“分布式”。

图 6.9 “新建对象-组”对话框

⑤ 单击“确定”按钮，完成域组的建立。

每个组账号添加完成后，系统都会为其建立一个唯一的安全识别码（SID），在 Windows Server 2003 系统内部都是利用 SID 来表示该组，有关权限的设置等都是通过 SID 来设置的。

可以先选择组账户，单击鼠标右键，并从弹出的快捷菜单中选择“重命名”命令，来更改组账户名。由于更改名称后，在 Windows Server 2003 内部的安全识别码（SID）并没有改变，因此，此组账户的属性和权限等设置都不变。

也可以先选择要删除的组账户，单击鼠标右键，并从弹出的快捷菜单中选择“删除”命令，将组账户删除。将账户删除后，即使添加一个相同名称的组账户（SID 不同），也不会继承前一个被删除账户的属性和权限等设置。

（2）添加组域的成员。要将用户账户和组加入到域组中，可以在“Active Directory 用户和计算机”对话框中双击域名或某组织单位，并在所选的域组上单击鼠标右键，并从弹出的快捷菜单中选择“属性→成员→添加”命令，选定要被加入的成员，如用户账户或组等，然后单击“添加”按钮，最后单击“确定”按钮，完成设置。

步骤 5：将计算机加入到域中

普通用户可以将自己使用的计算机加入到域中。

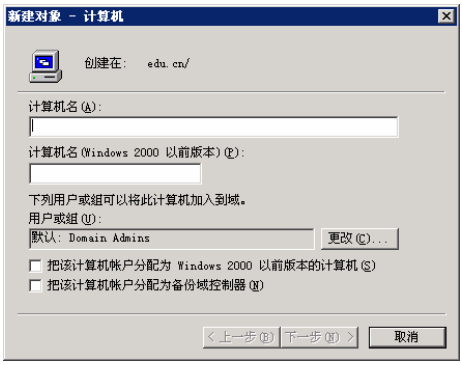

图 6.10 “新建对象-计算机”对话框

（1）管理员打开管理工具中的“Active Diretory 用户和计算机”，然后，打开“computer”，在空白区域右击，选择“新建→计算机”命令，打开“新建对象-计算机”对话框，如图 6.10 所示。

（2）单击“更改”按钮，打开“选择用户和组”对话框，在其中选择张三的用户账户 Zongjl，单击“确定”按钮。

（3）用户张三在自己的计算机上确认设置了正确的 DNS 服务器，然后打开系统属性对话框，更改主机名为“zongjl”，选择加入域“xpc.cn”，然后按照提示输入自己在域中的用户名和密码即可。

习 题

一、填空题

1．在域用户的属性设置中，用来设置用户只能在特定时间登录的属性是_____，用来设置用户只能在特定计算机上登录的属性是_____。

2．域采用集中式的管理方式，域中所有用户身份验证、权限管理等操作在_____上完成的，它是整个域的核心，简写为 DC。

二、简答题

1．什么是 Windows Server 2003 活动目录？它有什么特点？

2．什么是域控制器？什么是成员服务器？它们两者之间有什么关系？

3．在工作组中，用户账户存放在什么位置？

4．在域模式中，用户账户存放在什么位置？

三、实训题

1．在域中新建一个域用户 student，新建一个全局组 xxgcx，把 student 加入到全局组 xxgcx 中，并设置域用户只能在 8:30～11:30 登录。

2．在域中新建一个组织单位 xxgcx，将一个客户端计算机 computer 加入到组织单位中，并对该客户端计算机进行存储方面的管理。

项目 7　单位内部DNS架设及域名解析服务

7.1　项目内容

1．项目目的

在了解 DNS 工作原理整个工作过程的基础上，掌握在 Windows Server 2003 系统下 DNS 的安装和配置方法。

2．项目任务

有一所高等院校，要组建学校的校园网并架设单位内部的 Web 网站和 FTP 服务器，同时单位内部的计算机接入互联网。现需要安装并配置一台 DNS 服务器为校园网内部的用户提供 DNS 服务，使用户能够使用域名访问单位内部的 Web 网站、FTP 服务器和因特网上的各个网站。

3．任务目标

① 理解 DNS 的基本概念和工作原理；
② 理解 DNS 的解析过程；
③ 学会 DNS 服务器的安装方法；
④ 学会正向和反向查找区域的建立方法；
⑤ 学会 DNS 服务器的测试方法。

7.2　相关知识

7.2.1　hosts文件

因特网的前身 ARPA 网只为少量的计算机提供连接服务，用一个名为 hosts 的文本文件对网内的所有主机提供地址翻译。hosts 文件是一个纯文本文件，可用文本编辑器软件来处理，建立 IP 地址和名称（可以是域名、主机名或计算机名）的对照表，使用起来非常方便，例如：

10.8.10.250　www.abc.com　（域名）
10.8.10.251　Sales　　（名称）

现在的 TCP/IP 网络仍然支持这种传统方式。在本地主机上建立 hosts 文件后，要同某主机通信时，可直接使用该主机的名称，本地主机将该名称自动翻译成目标主机的 IP 地址。hosts 文件只适合小型的网络使用，对于大型的网络，为每个主机的 IP 地址都编入 hosts 文件是非常麻烦的，而且只要有主机更改名称或者 IP 地址时，每台主机都要更新，以保持 hosts 文件中名称和 IP 地址的一致性。因此，随着越来越多的主机加入网络，产生了一种基于分布式数据库的域名系统——DNS。

不过利用 hosts 文件寻找 IP 地址的效率比较高，特别适合于规模较小的内部互联网络。

注意 不同的操作系统，hosts 文件存放的目录不同。例如，在 Windows NT /2000 /XP / 2003 中，其文件名为 hosts，存放目录为操作系统安装目录（如 C:\winnt）下的子目录（\system32\drivers\etc）；而在 Windows 95/98/Me 系统上，其文件名为 hosts.sam，存放目录为操作系统安装目录（如 C:\windows），但在使用前还需将 hosts.sam 更名为 hosts。

7.2.2 域名系统

域名系统 DNS（Domain Name System）是一种采用客户/服务器（C/S）模式实现名称与 IP 地址转换的系统。整个 DNS 域名系统包括以下 4 个组成部分：

- DNS 域名称空间：指定用于组织名称的域的层次关系；
- 资源记录：将 DNS 域名映射到特定类型的资源信息，以供在名称空间中注册或解析名称时使用；
- DNS 服务器：存储和应答资源记录的名称查询；
- DNS 客户端：也称解析程序，用来查询 DNS 服务器，将名称解析为查询中指定的资源记录类型。

通过在 DNS 服务器端建立 DNS 数据库，记录主机名称与 IP 的对应关系，为客户端的主机提供 IP 地址解析服务。当某主机要与其他主机通信时，可利用主机名称向 DNS 服务器查询此主机的 IP 地址。

因特网上采用了层次树状结构的命名方法，如图 7.1 所示，如同一棵倒过来的树，层次结构非常清楚。根域位于最顶端，在根的下面是几个顶级域，每个顶级域又进一步划分为不同的二级域，二级域下面再划分子域，子域下面可以有主机，也可以再分子域，直到最后主机。例如，主机 www.microsoft.com 只有 3 个层次，其中 microsoft.com 是域名，www 是主机名，表明该主机是 Web 服务器；而主机 www.xpc.edu.cn 为四个层次，其中 xpc.edu.cn 是域名，www 为主机名。

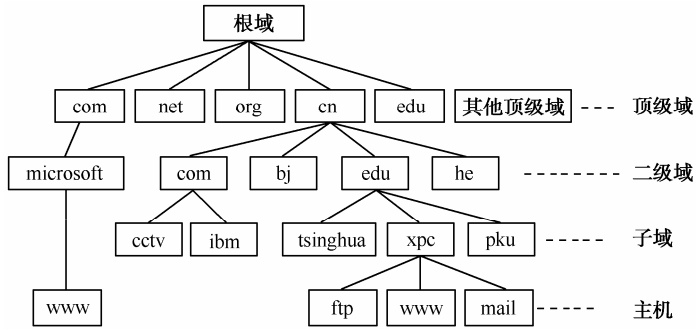

图 7.1 因特网的域名结构

与文件系统的结构类似，每个域可以用相对的或绝对的名称来标志。相对于父域来表示一个域，可以用相对域名；绝对域名指完整的域名。主机名是指为每台主机指定的主机名称，带有域名的主机名是全称域名。

ICANN 是因特网名字与编号分配机构，其前身是 InterNIC（国际因特网络信息中心）。ICANN 负责管理世界范围内的 IP 地址分配，也管理着整个域结构。整个因特网的域名服务

器都是由 DNS 来实现的。要在整个因特网范围内识别特定的主机，必须使用全称域名，如 xpc.edu.cn。在因特网中的每个网络都必须有自己的域名，应向 ICANN 注册自己的域名，这个域名对应自己的网络，注册的域名就是网络域名。拥有注册域名后，即可在网络内为特定主机或主机的特定应用程序服务，自行指定主机名或别名，如 ftp 等。

域名系统在 TCP/IP 网络上是通过 DNS 服务器提供 DNS 服务来实现的。DNS 服务器的数据库中保存着域名与 IP 地址的对应表。

7.2.3 域名服务器

域名服务器是整个域名系统的核心。域名服务器，严格地讲应该是域名名称服务器（DNS Name Server），保存着域名称空间中部分区域的数据。

因特网上的域名服务器是按照域名的层次来安排的，每一个域名服务器都只对域名体系中的一部分进行管辖。域名服务器有 3 种类型：

1．本地域名服务器

本地域名服务器（Local Name Server）也称默认域名服务器。当一个主机发出 DNS 查询报文时，这个报文就首先被送往该主机的本地域名服务器。在用户的计算机中设置网卡的“Internet 协议（TCP/IP）属性”对话框中设置的“首选 DNS 服务器”即为本地域名服务器。如图 7.2 所示。本地域名服务器离用户较近，一般不超过几个路由器的距离。当所要查询的主机也属于同一本地 ISP 时，该本地域名服务器会立即将所查询的主机名转换为它的 IP 地址，而不需要再去询问其他的域名服务器。

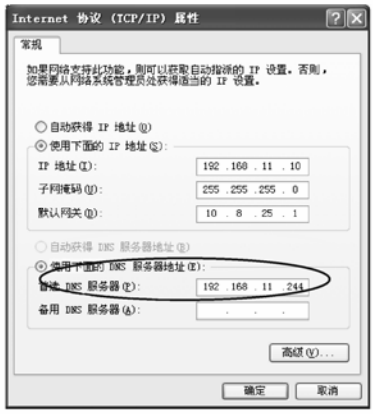

图 7.2 设置本地域名服务器

2．根域名服务器

目前因特网上有十几个根域名服务器（Root Name Server），大部分都在北美。当一个本地域名服务器不能立即回答某个主机的查询时，该本地域名服务器就以 DNS 客户的身份向某一根域名服务器查询。

若根域名服务器有被查询主机的信息，就发送 DNS 回答报文给本地域名服务器，然后本地域名服务器再回答给发起查询的主机。但当根域名服务器没有被查询主机的信息时，它一定知道某个保存有被查询主机名字映射的授权域名服务器的 IP 地址。通常根域名服务器用来管辖顶级域（如.com）。根域名服务器并不直接对顶级域下面所属的域名进行转换，但它一定能够找到所有二级域名的域名服务器。

3．授权域名服务器

每一个主机都必须在授权域名服务器处注册登记。通常，一个主机的授权域名服务器就是它的本地 ISP 的一个域名服务器。实际上，为了更加可靠地工作，一个主机最好有至少两个授权域名服务器。许多域名服务器同时充当本地域名服务器和授权域名服务器。授权域名服务器总是能够将其管辖的主机名转换为该主机的 IP 地址。

每个域名服务器都维护一个高速缓存，存放最近用过的名字及从何处获得名字映射信息的记录。当客户请求域名服务器转换名字时，服务器首先按标准过程检查它是否被授权管理

该名字。若未被授权，则查看自己的高速缓存，检查该名字是否最近被转换过。域名服务器向客户报告缓存中有关名字和地址的绑定（binding）信息，并标志为非授权绑定，以及给出获得此绑定的服务器 S 的域名。本地服务器同时也将服务器 S 与 IP 地址的绑定告知客户。因此，客户能够很快收到回答，但有可能信息已是过时的了。如果强调高效，客户可选择接受非授权的回答信息并继续进行查询；如果强调准确性，客户可与授权服务器联系，并检验名字与地址间的绑定是否仍有效。

因特网允许各个单位根据本单位的具体情况将本单位的域名划分为若干个域名服务器管辖区（Zone），一般就在各管辖区中设置相应的授权域名服务器。如图 7.3 所示，abc 公司有下属部门 x 和 y，部门 x 下面有 3 个分部门 u、v 和 w，部门 y 下面还有其下属的部门 t。

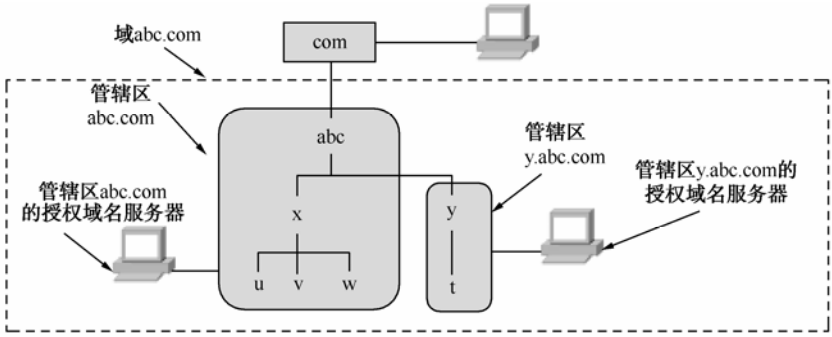

图 7.3　域名服务器管辖区的划分

7.2.4　域名的解析过程

1．DNS解析流程

当使用浏览器阅读网页时，在地址栏输入一个网站的域名后，操作系统会呼叫解析程序（即客户端负责 DNS 查询的 TCP/IP 软件），开始解析此域名对应的 IP 地址，其运作过程如图 7.4 所示。

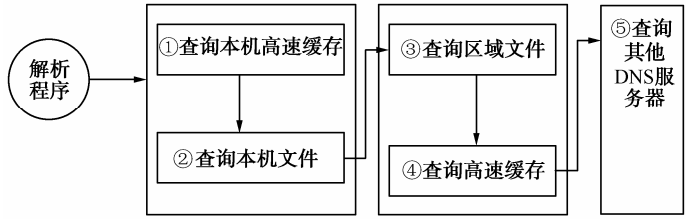

图 7.4　DNS 解析程序的查询流程

① 解析程序查询本机的高速缓存记录，如果从高速缓存内即可得知该域名所对应的 IP 地址，就将此 IP 地址传给应用程序。

② 如果在本机高速缓存中找不到答案，接着解析程序会查询本机文件 hosts.txt，看是否能找到相对应的数据。

③ 如果还是无法找到对应的 IP 地址，则向本机指定的域名服务器请求查询。域名服务器在收到请求后，会先检查此域名是否为管辖区域内的域名。

④ 如果在区域文件内找不到对应的 IP 地址，则域名服务器会检查本身所存放的高速缓存，看是否能找到相符合的数据。

⑤ 如果还是无法找到相对应的数据，就需要借助外部的域名服务器，这时就会开始进行域名服务器与域名服务器之间的查询操作。

上述 5 个步骤，可分为两种查询模式，即客户端对域名服务器的查询（第③、④步）及域名服务器和域名服务器之间的查询（第⑤步）。

1）递归型查询

DNS 客户端要求域名服务器解析 DNS 名称时，采用的多是递归型查询（Recursive Query）。当 DNS 客户端向 DNS 服务器提出递归型查询时，DNS 服务器会按照下列步骤来解析名称：

① 如果域名服务器本身的信息足以解析该项查询，则直接响应客户端其查询的名称所对应的 IP 地址；

② 如果域名服务器无法解析该项查询，会尝试向其他域名服务器查询；

③ 如果其他域名服务器也无法解析该项查询，则告知客户端找不到数据。

从上述过程可得知，当域名服务器收到递归型查询时，必然会响应客户端其查询的名称所对应的 IP 地址，或者是通知客户端找不到数据。

2）循环型查询

循环型查询多用于域名服务器与域名服务器之间的查询。它的工作过程是：当第 1 台域名服务器向第 2 台域名服务器（一般为根域服务器）提出查询请求后，如果在第 2 台域名服务器内没有所需要的数据，则它会提供第 3 台域名服务器的 IP 地址给第 1 台域名服务器，让第 1 台域名服务器直接向第 3 台域名服务器进行查询。以此类推，直到找到所需的数据为止。如果到最后一台域名服务器中还没有找到所需的数据，则通知第 1 台域名服务器查询失败。

3）反向型查询

反向型查询的方式与递归型和循环型两种方式都不同，它是让 DNS 客户端利用自己的 IP 地址查询它的主机名称。

反向型查询是依据 DNS 客户端提供的 IP 地址，来查询它的主机名。由于 DNS 域名与 IP 地址之间无法建立直接对应关系，所以必须在域名服务器内创建一个反向型查询的区域，该区域名称最后部分为 in-addr.arpa。

一旦创建的区域进入 DNS 数据库中，就会增加一个指针记录，将 IP 地址与相应的主机名相关联。例如，当查询 IP 地址为 192.168.11.250 的主机名时，解析程序将向 DNS 服务器查询 250.11.168.192.in-addr.arpa 的指针记录。如果该 IP 地址在本地域之外，DNS 服务器将从根开始，顺序解析域节点，直到找到 250.11.168.192.in-addr.arpa。

当创建反向型查询区域时，系统就会自动为其创建一个反向型查询区域文件。

2．DNS完整的查询过程

图 7.5 所示为一个包含递归型和循环型两种类型的查询方式，DNS 客户端向域名服务器 Serverl 查询 www.xpc.edu.cn 的 IP 地址的过程。查询的具体解析过程如下：

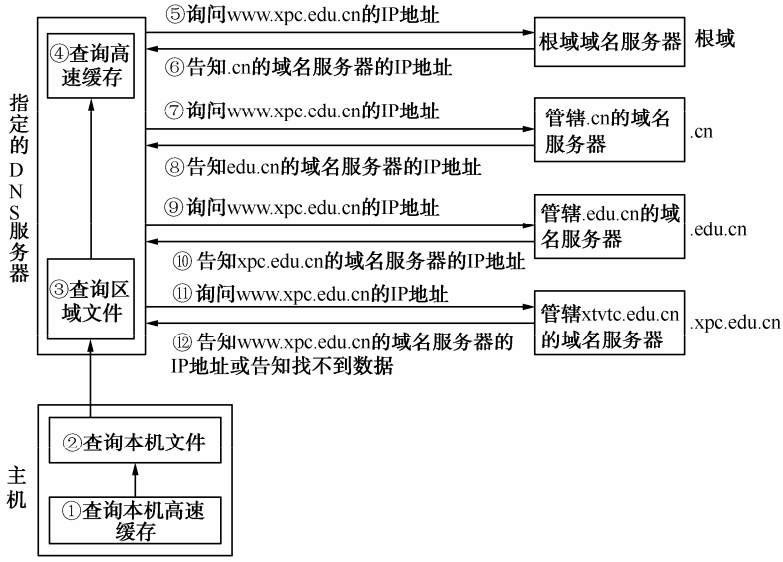

图 7.5　完整的 DNS 解析过程

域名解析使用 UDP 协议，其 UDP 端口号为 53。提出 DNS 解析请求的主机与域名服务器之间采用客户机/服务器（C/S）模式工作。当某个应用程序需要将一个名字映射为一个 IP 地址时，应用程序会调用一种名为解析器（resolver，参数为要解析的域名地址）的程序，由解析器将 UDP 分组传送给本地 DNS 服务器，由本地 DNS 服务器负责查找名字并将 IP 地址返回给解析器，解析器再把它返回给调用程序。本地 DNS 服务器以数据库查询方式完成域名解析过程，并且采用了递归型查询。

3．域名解析的效率

为了提高解析速度，域名解析服务提供了两种方式的优化：复制和高速缓存。

复制是指在每个主机上保留一个本地域名服务器数据库的副本。由于不需要任何网络交互就能进行转换，因此复制使得本地主机上的域名转换非常快。同时，它也减轻了域名服务器的计算机负担，使服务器能为更多的计算机提供域名服务。

高速缓存是比复制更重要的优化技术，它可使非本地域名解析的开销大大降低。网络中每个域名服务器都维护一个高速缓存器，由高速缓存器来存放用过的域名和从何处获得域名映射信息的记录。当客户机请求服务器转换一个域名时，服务器首先查找本地域名到 IP 地址映射数据库，如果无匹配地址，则检查高速缓存中是否有该域名最近被解析过的记录。如果有记录就返回给客户机，如果没有记录便应用某种解析方式或算法解析该域名。为保证解析的有效性和正确性，高速缓存中保存的域名信息记录设置有生存时间，这个时间由响应域名询问的服务器给出，超时的记录将从缓存区中删除。

7.2.5　对象类型和资源类型

在 Windows Server 2003 中，DNS 数据库中都会包含 DNS 服务器所使用的一个或多个区域文件，保存在\winnt\system32\dns 文件夹内，如 10.8.10.in-addr.arpa，xpc.edu.cn，可以使用文本编辑器打开。每个区域文件都由许多的资源记录所组成，包含许多对象类型。当设置 DNS 域名解析、反向解析及其他管理目的时，需要许多不同类型的资源记录，下面就介绍它们的

代表意义。

在因特网中，域名系统具有广泛的通用性。它既可以用于标志主机，也可以标志邮件交换。为了区分不同类型的对象，域名系统中的每一个条目都被赋予了“类型”（type）属性。这样，一个特定的名字就可能对应域名系统的若干个条目。表 7.1 列出了域名系统的对象类型。

表 7.1　域名系统的对象类型

类　型	意　义	内　容
SOA	授权开始	标志一个资源记录集合（称为授权区段）的开始
A	主机地址	IP 地址（标志一个主机名与其所对应的 IP 地址的映射）
MX	邮件交换	邮件服务器名及优先级（标志一个邮件服务器与其所对应的 IP 地址的映射）
NS	域名服务器	域的授权名字服务器
CNAME	别名	其他的规范名字
PTR	指针	对应于 IP 地址的主机名
SRV	服务	用来记录提供特殊服务的服务器的相关数据
HINFO	主机描述	ASCII 字符串，用于 CPU 和 OS 描述
TXT	文本	ASCII 字符串

（1）授权开始（Start of Authority，SOA）记录。授权开始记录用于记录该区域内主要名称服务器（即保存该区域数据正本的 DNS 服务器）与此区域管理者的电子邮件账号。当新建一个区域后，SOA 会被自动创建，所以 SOA 是区域内第 1 个记录文件。如在 xpc.edu.cn 文件中：

```
[区域名称] [TTL 时间] IN SOA 主要服务器名称 管理员 E-mail（
区域版本编号
同步更新时间
同步重试时间
同步到期时间
TTL 默认值）
@                    IN  SOA xxzx-chujl2000.  admin. （
                     13          ; serial number
                     900         ; refresh
                     600         ; retry
                     86400       ; expire
                     3600      ) ; minimum TTL
```

（2）主机（A Host）记录。主机记录，也叫做 A 记录，是用来静态地建立主机名与 IP 地址之间的对应关系，以便提供正向查询的服务。

主机记录将主机名（如上例的 www、mail）与一个特定的 IP 地址联系起来。

```
[主机名] [TTL 时间] AIP 地址
host                 A   192.168.11.250
```

（3）邮件交换（Mail Exchanger，MX）记录。邮件交换记录可以告诉用户哪些服务器可

以为该域接收邮件。接收邮件的服务器一般是专用的邮件服务器，也可以是一台用来转送邮件的主机。每一个 MX 记录有两个参数：preference 和 mailserver。

当用户在局域网内部传送邮件时（邮件的后辍为@abc.net），一般可由局域网内部的邮件服务器完成交换；当用户需要向局域网之外的其他因特网用户发送邮件时，则通过指向 ISP 的邮件服务器进行交换。

（4）域名服务器（Name Server，NS）记录。域名服务器记录用于记录管辖此区域的名称服务器，包括主要名称服务器和辅助名称服务器，这样就允许其他域名服务器到该域查找域名。一个区域文件可能有多个域名服务器记录。

（5）别名（Canonial Name 或 CNAME）记录。别名记录用来记录某台主机的别名。别名记录在平时的应用中很有用，它可以给一台主机设置多个别名，每一个别名代表一个应用。例如，有一个名为 host.xpc.edu.cn 的主机，它同时可以有多个别名，一个为 mail.xpc.edu.cn，用于邮件服务；另一个为 ftp.xpc.edu.cn，用于 FTP 服务；还可以再有一个为 www.xpc.edu.cn，用于因特网服务。也就是说，这几台不同名称的主机返回的 IP 地址完全相同。

```
[主机别名] [TTL 时间] CNAME 主机名
mail                  CNAME   host.xpc.edu.cn.
www                   CNAME   host.xpc.edu.cn.
```

（6）指针（PTR）记录。主机记录将一个主机名映射到一个 IP 地址上；而指针记录则正好相反，它是将一个 IP 地址映射到一个主机上。指针记录为反向型查询提供了条件，用户有时要求 DNS 服务器找出与一个特定地址相对应的 FQDN，这是一个很有用的功能，这可以防止某些非法用户用伪装的或不合法的域名来使用 E-mail 或 FTP 服务。

```
主机 IP 地址   [TTL 时间]   IN PTR   主机名称
250                   PTR host.xpc.edu.cn.
251                   PTR host.dzx.xpc.edu.cn.
```

（7）服务（SRV）记录。服务记录用来记录提供特殊服务的服务器的相关数据。例如，它可以记录域控制器的完整的计算机名与 IP 地址，使客户端登录时可以通过此记录寻找域控制器，以便审核登录者的身份。

7.3 方案设计及准备

1．设计

某高等院校建立校园网后需要为单位的内部局域网提供 DNS 服务，使用户能够使用域名访问内部的计算机和网站。

配置 Windows Server 2003 系统下的 DNS 服务管理，如图 7.6 所示的阴影部分。

（1）服务器端：在一台计算机上安装 Windows Server 2003 系统，设置 IP 地址为 192.168.11.244，子网掩码为 255.255.255.0；设置主机域名与 IP 地址的对应关系，host.xpc.edu.cn 对应 192.168.11.250/24，邮件服务器 mail.xpc.edu.cn 对应 192.168.11.250，文件传输服务器 ftp.xpc.edu.cn 对应 192.168.11.250，host.dzx.xpc.edu.cn 对应 192.168.11.251；设置 host.xpc.edu.cn 别名为 www.xpc.edu.cn，设置 host.dzx.xpc.edu.cn 别名为 www.dzx.xpc.edu.cn；设置转发器为 202.99.160.68。

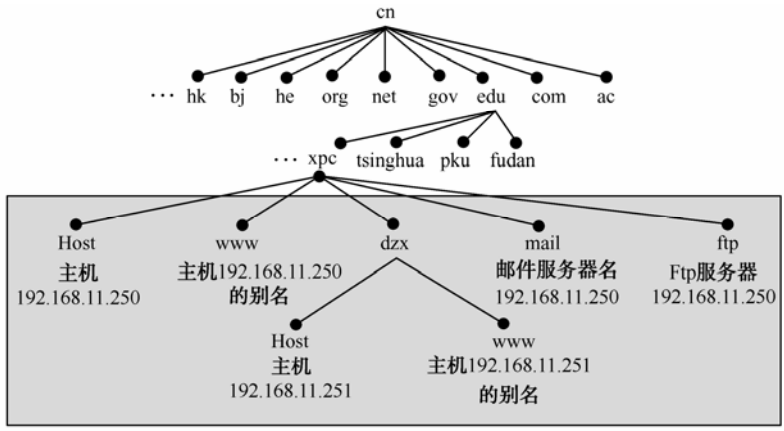

图 7.6　阴影部分为 DNS 服务管理部分的因特网的域名结构

（2）客户端：设置 DNS 客户端计算机 PCA 的 IP 地址为 192.168.11.10/255.255.255.0，PCB 的 IP 地址为 192.168.11.11/255.255.255.0，两台计算机的 DNS 服务器为 192.168.11.244，启用客户端计算机的 IE 浏览器，访问 www.xpc.edu.cn、mail.xpc.edu.cn 和 www.dzx.xpc.edu.cn。

（3）在 DOS 环境下，通过“ping 域名”命令可以将域名解析为 IP 地址。试用 ping 解析 www.sina.com.cn 、 www.263.net 、 www.yahoo.com.cn 、 www.xpc.edu.cn 、 mail.xpc.edu.cn 、 www.dzx.xpc.edu.cn、www.sohu.com 等主机对应的 IP 地址。

根据以上要求，本项目实施的网络拓扑图如图 7.7 所示。

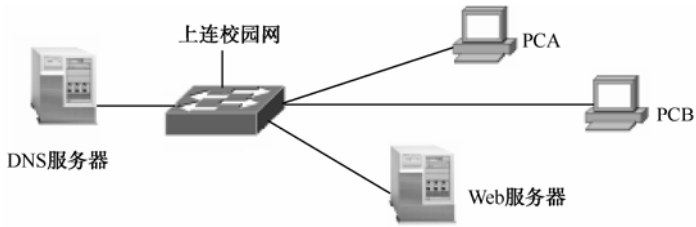

图 7.7　DNS 配置网络拓扑图

2．设备清单

为了搭建图 7.7 所示的网络环境，需要如下设备：

① 安装 Windows Server 2003 系统的计算机 2 台，一台用做 DNS 服务器，一台用做 Web 服务器。

② 安装 Windows XP 系统的计算机 2 台，并已连入校园网。

7.4　项目实施

步骤 1：硬件连接

按照图 7.7 所示拓扑，搭建 DNS 服务器配置网络模型。

步骤 2：设置IP地址及测试连通性

设置各计算机的 IP 地址、子网掩码、网关，如表 7.2 所示。

表 7.2　各计算机的 IP 地址、子网掩码与网关

计算机	IP 地址	子网掩码	网关
DNS 服务器	192.168.11.244	255.255.255.0	192.168.11.1
Web 服务器	192.168.11.250	255.255.255.0	192.168.11.1
PCA	192.168.11.10	255.255.255.0	192.168.11.1
PCB	192.168.11.11	255.255.255.0	192.168.11.1

使用 ping 命令测试各计算机之间的连通性。如果全通则继续进行，否则检测网线及计算机的配置，直到各计算机之间全部连通。

步骤 3：安装DNS服务器

如果在“开始→程序→管理工具”选项中找不到“DNS”选项，就需要自行安装 DNS 服务器。通过“添加和删除应用程序”来安装，安装过程与 DHCP 服务安装大致相同，在这里不再详细介绍。

安装完毕后，在管理工具中多了一个“DNS”控制台。在安装活动目录的同时也安装和配置了 DNS 服务器。

步骤 4：设置DNS服务器

在有 DNS 服务的 Windows Server 2003 服务器中，配置满足设计要求 1 的 DNS 服务器，步骤如下：

（1）启动 Windows Server 2003 服务器，选择“开始→程序→管理工具→DNS”命令，进行 DNS 管理与配置。

（2）在 DNS 管理与配置窗口中加入需要管理和配置的域名服务器。右击“树”区域的“DNS”选项，在弹出的菜单中选择“连接到 DNS 服务器”选项，弹出“连接到 DNS 服务器”对话框，如图 7.8 所示。Windows Server 2003 中的 DNS 管理程序既可以管理和配置本地的域名服务，也可以管理和配置网络中其他主机的 DNS。选择“这台计算机”，单击“确定”按钮，系统将把这台计算机（计算机名为 xxzx-chujl）加入到 DNS 树中，如图 7.9 所示。这时就在该计算机上建立一个数据库，用于存储授权区域的域名信息。

（3）在“xxzx-chujl”下包括“事件查看器”、“正向查找区域”、“反向查找区域”3 个选项。

步骤 5：建立正向查找区域

DNS 客户端所提出的 DNS 查找请求，大部分是属于正向查找，也就是从主机名称来查找 IP 地址。建立步骤如下：

（1）选择“开始→程序→管理工具→DNS”命令，然后选择“DNS 服务器”并右击“正向查找区域”选项，在弹出的菜单中选择“新建区域”选项，启动“欢迎使用新建区域”向导。单击“下一步”，弹出“区域类型”对话框，如图 7.10 所示。

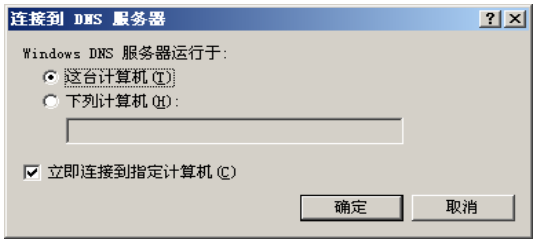

图 7.8 “连接到 DNS 服务器”对话框

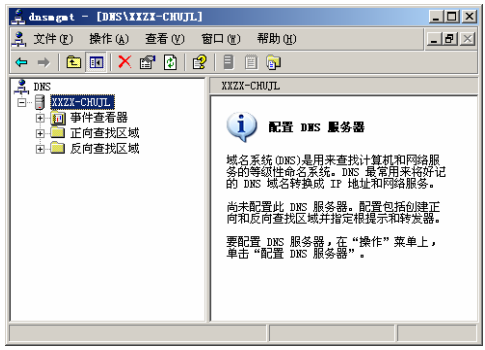

图 7.9 加入本机后的 DNS 管理与配置界面

（2）选择“主要区域”单选按钮，单击“下一步”按钮，弹出“区域名称”对话框，如图 7.11 所示。在“区域名称”文本框中输入区域名“xpc.edu.cn”，注意只输入到次级域，而不是连同子域和主机名称都一起输入。

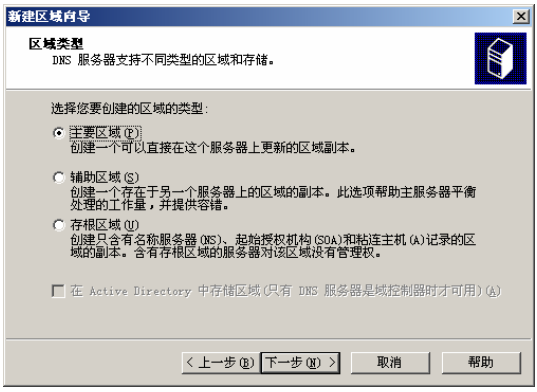

图 7.10 “区域类型”对话框

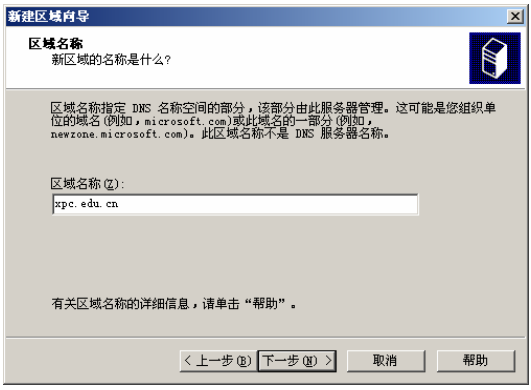

图 7.11 “区域名称”对话框图

（3）单击“下一步”按钮，弹出“区域文件”对话框，如图 7.12 所示。在“创建新文件，文件名为”文本框中自动输入了域名为文件名的 DNS 文件。该文件的默认文件名为 xpc.edu.cn.dns（区域名+.dns），它被保存在\winnt\system32\dns 文件夹中。如果要使用区域内已有的区域文件，可先选择“使用此现存文件”项，然后将该现存的文件复制到\winnt\system32\dns 文件夹中。

（4）单击“下一步”按钮，弹出“动态更新”对话框，如图 7.13 所示。选择“允许非安全和安全动态更新”选项表示任何客户端接受资源记录的动态更新，该设置存在安全隐患。选择“不允许动态更新”选项，表示不接受资源记录的动态更新，更新记录必须手动。

（5）单击“下一步”按钮，单击“完成”按钮。新区域“xpc.edu.cn”添加到 DNS 管理窗口。

在 Windows Server 2003 的 DNS 允许建立以下 3 种类型的区域。

（1）主要区域（Primary Zone）：用来存储此区域内所有记录的正本。在 DNS 服务器内建立主要区域后，可以直接在此区域内新建、修改和删除记录。区域内的记录可以存储在文件或 Active Directory 数据库中。

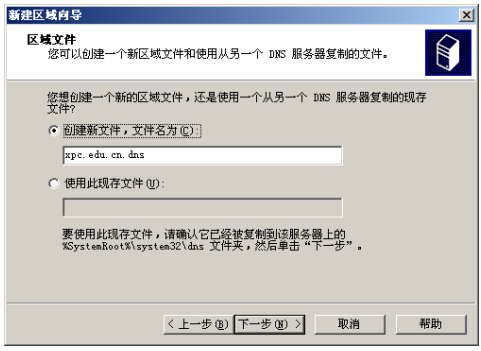

图 7.12 “区域文件”对话框

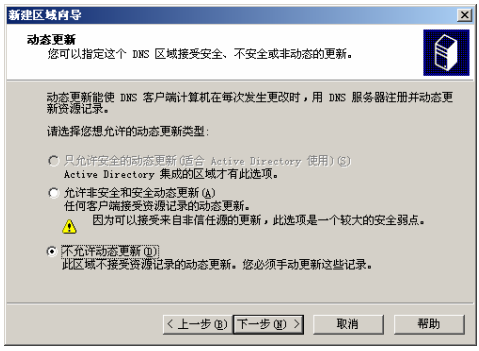

图 7.13 “动态更新”对话框

- 如果 DNS 服务器是独立服务器或成员服务器，则区域内的记录存储在“区域文件”内，文件名默认为“区域名称.dns”，存储在%systemboot%\system32\dns 文件夹内，类型为文本文件。
- 如果 DNS 服务器是域控制器，则可以记录存储在“区域文件”或 Active Directory 数据库内。若将其存储到 Active Directory 数据库内，则此区域被称为“Active Directory 整合区域”，此区域内的记录会随着 Active Directory 数据库的复制动作，自动被复制到其他的域控制器。

（2）辅助区域（Secondary Zone）：辅助区域内的每一项记录都存储在“区域文件”中，存储区域内所有记录的副本，是利用“区域复制”从其“master 服务器”复制过来的。辅助区域内的记录是只读的、不可修改的。

（3）存根区域（Stub Zone）：存储着一个区域的副本信息，不过它与辅助区域不同，存根区域只包含少量记录（如 SOA 、NS），利用这些记录可以找到此区域的授权服务器。

步骤 6：在主要区域内新建资源记录

DNS 服务器支持相当多的不同类型的资源记录，下面介绍如何将几个比较常用的资源记录新建到区域内。

1）新建一项主机记录

将主机名称与 IP 地址（也就是资源记录类型为 A 的记录）新建到 DNS 服务器内的区域后，就可以让 DNS 服务器提供这台主机的 IP 地址给客户端。

① 右击欲新增加记录的区域名，如 xpc.edu.cn，在弹出的菜单中选择“新建主机”选项。弹出“新建主机”对话框，如图 7.14 所示。

② 在“名称”栏中填写新增主机记录的名称，但不需要填上整个域名，如要新增 host 名称，只要填上 host 即可，而不需填上 host.xpc. edu.cn。在“IP 地址”栏中填入欲新建名称的实际 IP 地址，如 192.168.11.250。如果 IP 地址与 DNS 服务器在同一个子网掩码下，并且有反向查找区域，则可以选择“创建相关的指针（PTR）记录”，这样会在反向查找区域自动添加一项搜索记录。单击“添加主机”按钮，该主机的名字、对象类型及 IP 地址就显示在 DNS 管理窗口中。如图 7.15 所示。

图 7.14　“新建主机”对话框

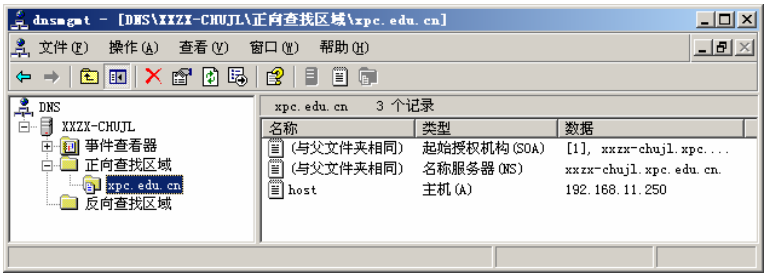

图 7.15　添加主机后的 DNS 管理窗口

可以重复以上步骤，将多台主机的信息输入到此区域内。

2）新建一项主机别名

如果想要让一台主机拥有多个主机名称，可以为该主机设置别名。例如，一台主机 host.xpc.edu.cn 作为 Web 服务器时名称为 www.xpc.edu.cn，而作为 FTP 服务器时名称为 ftp.xpc.edu.cn，但这都是同一 IP 地址的主机。

右击欲新建立别名主机的区域名，如 xpc.edu.cn，在弹出的菜单中选择“新建别名”选项。弹出“新建资源记录”对话框，如图 7.16 所示，在“别名”文本框中输入主页服务器的名字“www”，然后输入目标主机的完全合格的域名 host.xpc.edu.cn（也可以通过单击“浏览”按钮进行选择），单击“确定”按钮，完成别名配置。同样方法创建别名“ftp”。图 7.17 所示为完成后的画面，它表示 host.xpc.edu.cn 的别名是 www.xpc.edu.cn 和 ftp.xpc.edu.cn.。

3）新建一项邮件交换器

将邮件送到邮件交换服务器（SMTP Server）后，邮件交换服务器必须将邮件转发到目的地的邮件交换服务器，邮件交换服务器通过向 DNS 服务器查找 MX 资源记录来得知目的地的邮件交换服务器。MX 记录着负责域邮件传送的交换服务器，如图 7.18 所示。

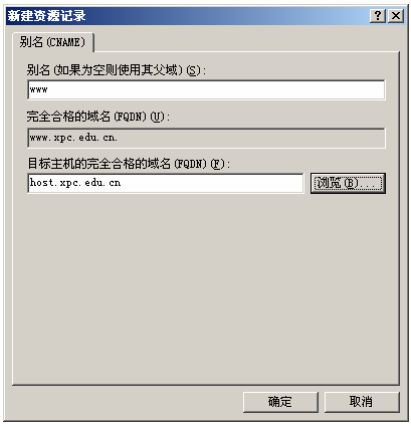

图 7.16 “新建资源记录”对话框

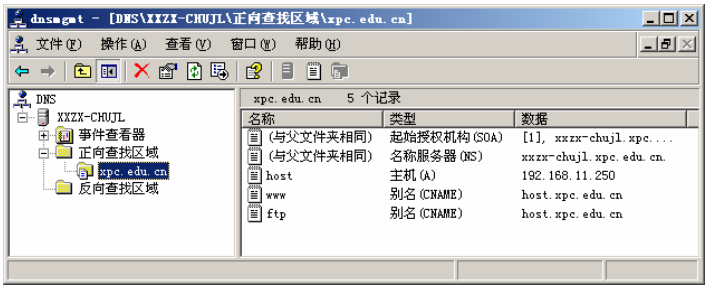

图 7.17 新建一项主机的别名

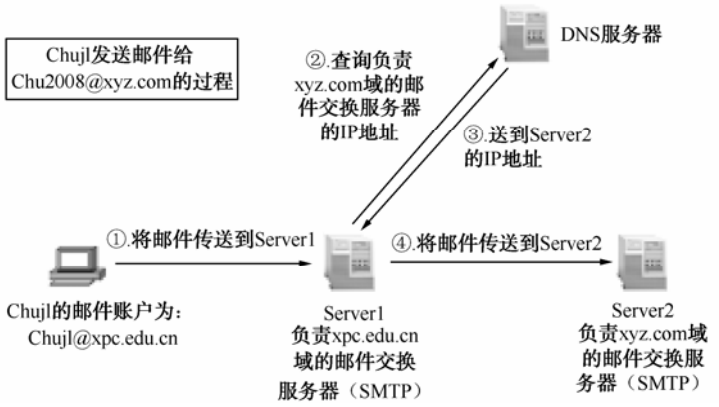

图 7.18 查找目的地邮件服务器的过程

右击 DNS 树中的区域名“xpc.edu.cn”，在弹出的菜单中选择“新建邮件交换器”选项。弹出“新建资源记录”对话框，如图 7.19 所示。

图 7.19 “新建资源记录”对话框

主机或子域：若输入 mail，则表示是在设置 mail.xpc.edu.cn 域的邮件交换服务器；若未

输入，则以“父域（parent domain）”为其负责的域，比如图 7.19 中的域 xpc.edu.cn。

邮件服务器的完全合格的域名（FQDN）：输入负责上述域邮件传送工作的邮件服务器的完整主机名称（FQDN），这台主机必须有一项类型为 A 的资源记录，以便得知其 IP 地址。

邮件服务器优先级：如果此域中有多台邮件交换服务器，则可以建立多个 MX 资源记录，并通过此处设置其优先级，数字较低的优先级较高（0 为最高）。

单击“确定”按钮，邮件服务器的名字、对象类型及指向的主机就显示在 DNS 管理窗口中。

步骤 7：建立反向区域

建立反向查找区域后可以让 DNS 客户端使用 IP 地址来查询主机名称。反向区域并不是必需的，可以在需要时创建。在 Windows Server 2003 中，DNS 分布式数据库是以名称为索引而非以 IP 地址为索引的。反向区域的前半部分是网络 ID（network ID）的反向书写，后半部分必须是.in-addr.arpa。例如，要查询网络 ID 为 192.168.11.250 的主机，则其反向区域前半部分的网络 ID 为 192.168.11，后半部分是.in-addr.arpa，区域文件为 11.168.192.in-addr.arpa.dns。

1）建立反向区域

① 建立反向查找区域与建立正向查找区域一样，右击“反向查找区域”选项，在弹出的菜单中选择“新建区域”选项，弹出“新建区域向导”对话框，单击“下一步”按钮，弹出“区域类型”对话框，选择“主要区域”选项，单击“下一步”按钮，弹出“反向查找区域名称”对话框，如图 7.20 所示，在“网络 ID”文本框中输入正常的地址（如 192.168.11.），这时会自动在反向查找区域名称中显示 11.168.192.in-addr.arpa。

② 单击“下一步”按钮，弹出“区域文件”对话框，在 “新文件”文本框中自动输入了以反向查找区域名为文件名的 DNS 文件。

③ 单击“下一步”按钮，选择“不允许动态更新”选项，单击“下一步”按钮，单击“完成”按钮，完成设置。反向查找区域自动添加在 DNS 管理窗口中，如图 7.21 所示。

2）在反向区域内建立记录

在反向区域内建立记录有两种方法，以便为 DNS 客户端提供反向查找的服务。

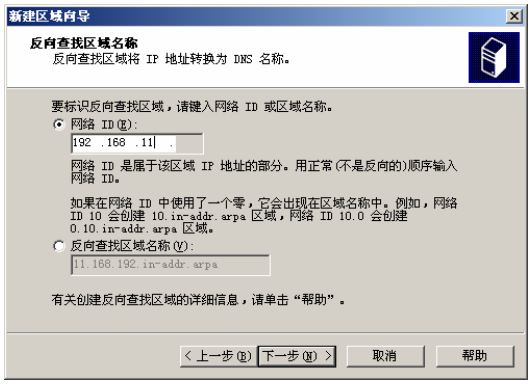

图 7.20 “反向查找区域名称”对话框

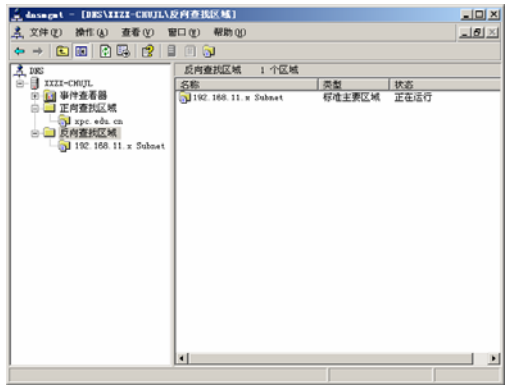

图 7.21 DNS 管理窗口

① 在图 7.21 中右击反向查找区域，然后选择“新增指针”选项。弹出“新建资源记录”对话框，如图 7.22 所示。在“主机 IP 号”中输入主机的 IP 地址的最后一组，如 250，在“主机名”文本框中输入指针指向的域名，如 host.xpc.edu.cn，也可以单击“浏览”按钮查找。

② 在正向区域建立主机记录时，可以顺便在反向区域内建立一项反向记录，在图 7.14 中勾选“创建相关的指针（PTR）记录”选项即可。但在选择此选项时，相对应的反向查找区域必须已经存在，例如，反向区域 192.168.11.x 子网必须已经存在。

图 7.22　新建指针

步骤 8：建立子域与委派域

如果 DNS 服务器所管辖的区域为 xpc.edu.cn，而且在此区域下还有数个子域，例如 dzx.xpc.edu.cn，则将子域内的记录建立到 DNS 服务器的方法有以下两种：

可以直接在 xpc.edu.cn 区域之下建立子域，然后将此子域内的主机记录输入到此子域内，这些记录还是存储在这台 DNS 服务器内的。

可以将子域内的记录委派给其他的 DNS 服务器来管理，也就是此子域内的所有记录都是存储在被委派的 DNS 服务器内的。

1）建立子域及其记录

为了管理图 7.6 中的 dzx 节点，需要在“xpc.edu.cn”之下再建立一个子域。

① 右击 DNS 树中的“xpc.edu.cn”，在弹出的菜单中执行“新建 DNS 域”命令，弹出“新建 DNS 域”对话框，如图 7.23 所示，在“请键入新的 DNS 域名”文本框中输入子域名“dzx”，单击“确定”按钮，dzx 将显示在区域“xpc.edu.cn”之下。

图 7.23　新建子域

② 在 dzx 子域中新建主机记录，右击子域名 dzx，在弹出的菜单中选择“新建主机”选项，弹出“新建主机”对话框，如图 7.24 所示，在“名称”文本框中输入新建主机的名称，如 host，在“IP 地址”栏中填入欲新建名称的实际 IP 地址，如 192.168.11.251，单击“添加主机”按钮，该主机的名字、对象类型及 IP 地址就显示在 DNS 管理窗口中。

图 7.24　子域内新建主机记录

③ 在 dzx 子域中新建别名，右击子域名 dzx，在弹出的菜单中选择“新建别名”选项，如图 7.25 所示。弹出“新建资源记录”对话框，在“别名”文本框中输入主页服务器的名字“www”，然后输入目标主机的完全合格的域名 host.dzx.xpc.edu.cn（也可以通过单击“浏览”按钮进行选择），单击“确定”按钮完成别名配置。图 7.26 为完成后的画面。

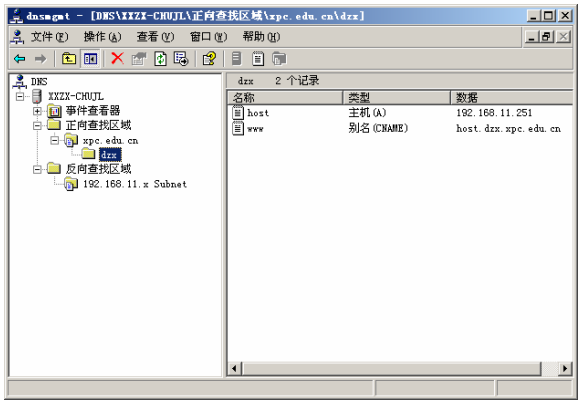

图 7.25　“新建资源记录”对话框

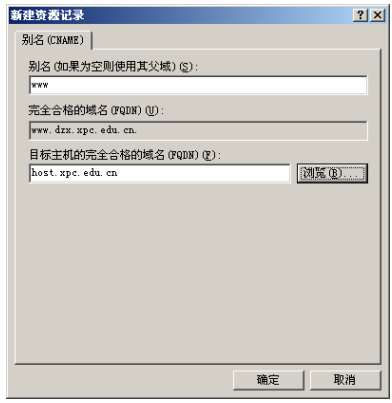

图 7.26　子域新建别名

2）扩展技能：DNS 泛域名解析

企业在 Web 服务器上为很多员工建立了个人网站，为了节省费用，采用虚拟主机技术，即在同一台服务器上架设多个网站，员工使用二级域名访问这些站点。然而，维护这些二级域名的工作量非常大，因此，采用 DNS 泛域名解析技术来解决这个难题。

① 在 DNS 管理控制台中，右击正向查找区域“xpc.edu.cn”，选择“新建域”命令，打开“新建 DNS 域”对话框，在“请键入新的 DNS 域名”文本框中输入“*”。

② 单击“确定”按钮，成功建立了一个子域，子域名为“*.xpc.edu.cn”，如图 7.27 所示。

③ 右击“*”区域，选择“新建主机”命令，打开“新建主机”对话框，如图 7.28 所示。

主机名留空，IP 地址为 Web 服务器的 IP 地址。

④ 单击“添加主机”按钮，成功添加一条主机记录；最后单击“完成”按钮。

操作完成后，可以在客户机上用“ping”命令进行验证。发现无论输入诸如“dzx.xpc.edu.cn”、“jdx.xpc.edu.cn”等域名，都会解析到主机“192.168.11.251”，实现了 DNS 泛域名解析。

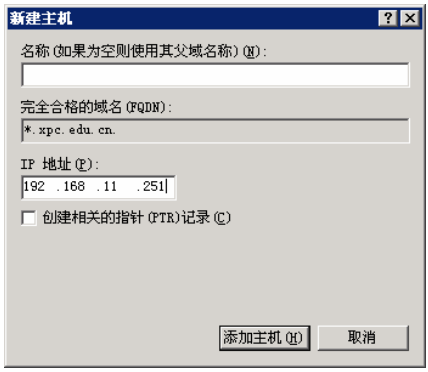

图 7.27　DNS 管理控制台窗口

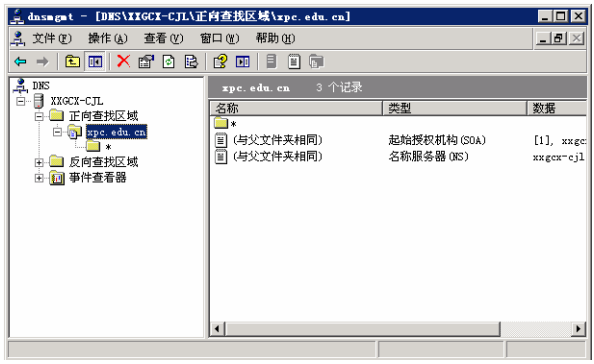

图 7.28　子域“新建主机”对话框

3）委派域

下面我们假设在 DNS 服务器 Server1 内有一个受管辖的区域 xpc.edu.cn，在此区域下新建一个子域（区域）qcx，并且要将此子域委派给另外一台 DNS 服务器 Server2 来管理，也就是此子域 qcx.xpc.edu.cn 内的所有记录都是存储在被委派的 DNS 服务器 Server2 内。当 Server1 收到查找 qcx.xpc.edu.cn 内的记录的请求时，Server1 会向 Server2 查找（查找模式为循环查询）。

操作步骤如下。

① 在 DNS 服务器 Server2 内建立区域 qcx.xpc.edu.cn，步骤见前所述。

② 在 DNS 服务器 Server1 上，右击区域 xpc.edu.cn，在弹出的菜单中选择“新建委派”选项，弹出“欢迎使用新建委派向导”对话框，单击“下一步”按钮，弹出“受委派域名”对话框，如图 7.29 所示，在“委派的域”文本框中输入被委派的域名，如 qcx。

③ 单击“下一步”按钮，弹出“名称服务器”对话框，单击“添加”按钮，弹出“新建资源记录”对话框，如图 7.30 所示。通过单击“浏览”按钮选择受委派的 DNS 服务器，如 host.xpc.edu.cn，单击“确定”按钮回到“名称服务器”对话框，此时刚才添加的受委派的 DNS 服务器已经添加进去。

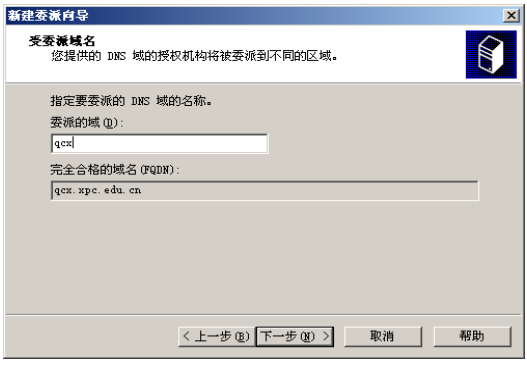

图 7.29　添加受委派的 DNS 服务器

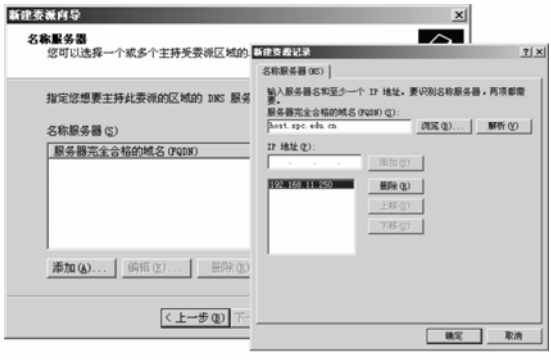

图 7.30　“新建资源记录”对话框

④ 单击“下一步”按钮，完成配置。如图 7.31 所示。其中 qcx 就是刚才委派的子域，其内只有一项 NS 的记录，它记载着 qcx.xpc.edu.cn 的授权服务器是 host.xpc.edu.cn。当 Server1 收到所有查询位于 qcx.xpc.edu.cn 内的记录的请求时，Server1 会向 Server2 查找。

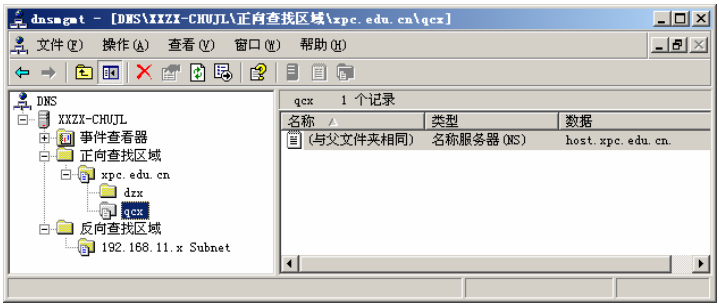

图 7.31　受委派子域中的 NS 项

步骤 9：建立辅助区域

辅助区域用来存储此区域内所有记录的副本，这份信息是从 master 服务器利用“区域复制”的方式复制过来的。

在 DNS 服务器 Server2（IP 地址为 192.168.11.245）上新建一个提供正向查找服务的辅助区域。这个区域是从 DNS 服务器 Server1 内的主要区域 xpc.edu.cn 复制过来的。

（1）在 master 服务器（Server1，IP 地址为 192.168.11.244）上确认将 xpc.edu.cn 区域复制到 Server2。右击 Server1 的 xpc.edu.cn 区域，选择“属性”选项，弹出“xpc.edu.cn 属性”对话框，选择“区域复制”标签，如图 7.32 所示。选择“到所有服务器”或选择“只允许到下列服务器”单选按钮，然后输入 Server2 的 IP 地址，如 192.168.11.245。

（2）到 DNS 服务器 Server2 上，右击“正向查找区域”，选择“新建区域”选项，弹出“欢迎使用新建区域向导”对话框，单击“下一步”按钮，弹出“区域类型”对话框，选中“辅助区域”单选按钮，然后输入与 master 服务器相同的区域名称，如 xpc.edu.cn。

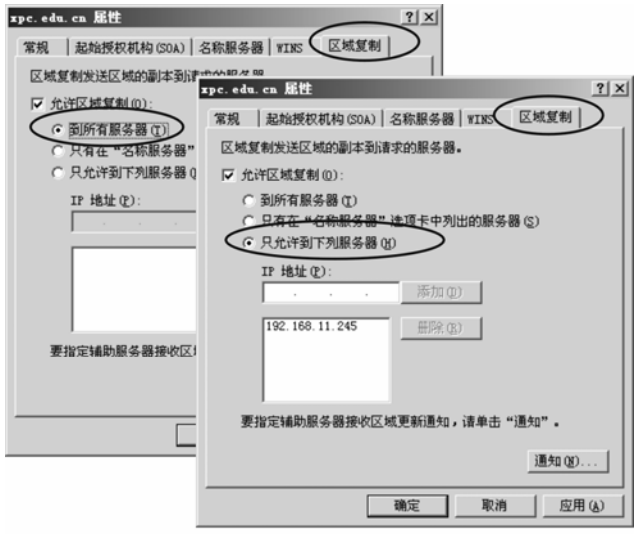

图 7.32　“xpc.edu.cn 属性”对话框

（3）单击“下一步”按钮，弹出“主 DNS 服务器”对话框，在 IP 地址栏中输入 master 服务器的 IP 地址，如 192.168.11.244，如图 7.33 所示，单击“添加”按钮，单击“下一步”按钮，完成配置。

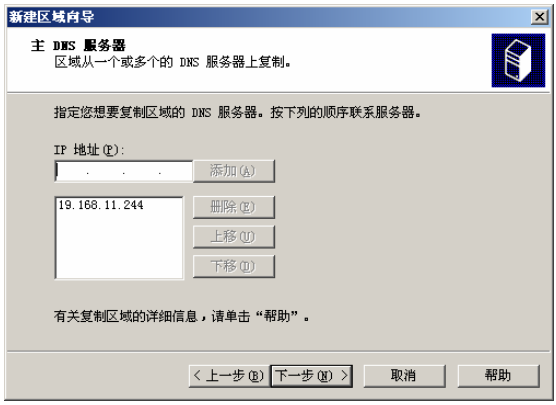

图 7.33 “主 DNS 服务器”对话框

存储复制区域的 DNS 服务器，默认每隔 15 分钟会自动向其 master 服务器请求执行“区域复制”操作。

（4）右击“辅助区域”，选择“从主服务器复制”或“从主服务器重新加载”的方式来手工执行“区域复制”。

步骤 10：建立存根区域

存根区域与委派域有点类似，但是此区域内只包含少数记录（如 SOA、NS 等记录），利用这些记录来寻找此区域的授权服务器。存根区域内的记录是从其 master 服务器复制过来的，而委派域内的 NS 记录是在执行委派动作时建立的，以后若此域有新的授权服务器，需要系统管理员手工添加。

假设在 DNS 服务器 Server2（IP 地址为 192.168.11.245）上新建一个正向的存根区域 xpc.edu.cn，此 xpc.edu.cn 的授权服务器是 Server1（IP 地址为 192.168.11.244）。当 Server1 收到查找 xpc.edu.cn 内的记录时，Server2 会向 Server1 查找（查找模式为循环查询）。

（1）在 master 服务器 Server1 内已经建立了区域 xpc.edu.cn。右击区域“xpc.edu.cn”，选择“属性”选项，弹出“xpc.edu.cn 属性”对话框，选择“区域复制”标签，如图 7.32 所示。选择“到所有服务器”或选择“只允许到下列服务器”单选按钮，然后输入 Server2 的 IP 地址，如 192.168.11.245。

（2）在 DNS 服务器 Server2 上，建立存根区域。右击“正向查找区域”，选择“新建区域”，弹出“欢迎使用新建区域向导”对话框，单击“下一步”按钮，弹出“区域类型”对话框，选择“存根区域”单选按钮，然后输入与 master 服务器相同的区域名称，如 xpc.edu.cn。

（3）其余步骤与建立辅助区域类似。

步骤 11：域的设置

通过右击区域选择“属性”选项，可以更改区域的相关设置，主要有：

1）更改区域类型与区域文件名称

右击 DNS 服务器的 xpc.edu.cn 区域，选择“属性”选项，弹出“xpc.edu.cn 属性”对话

框，选择“常规”标签，单击“更改”可以更改区域类型，在“区域文件名”栏中可以更改区域文件名称。如图 7.34 所示。

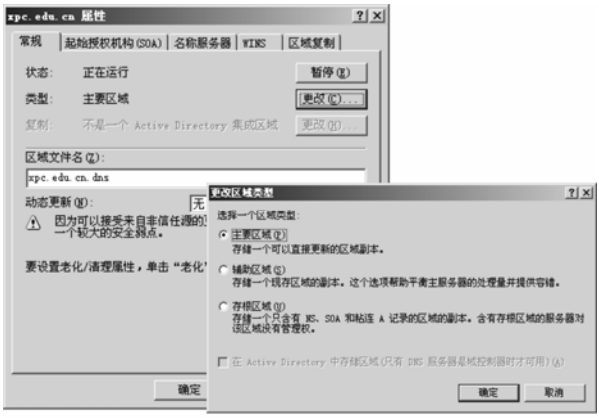

图 7.34　“xpc.edu.cn 属性”对话框

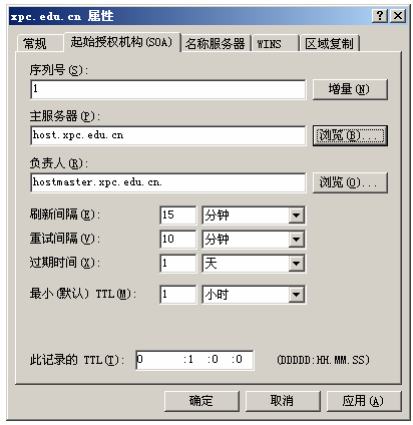

图 7.35　“起始授权机构”对话框

2）SOA 与区域复制

DNS 服务器的辅助区域存储的是此区域内所有记录的副本，这份副本信息是利用“区域复制”的方式从“master 服务器”复制过来的，“区域复制”执行的时间间隔的设置值存储在 SOA 资源记录内，在 master 服务器上，右击 DNS 服务器的区域，如 xpc.edu.cn，选择“属性”选项，弹出“xpc.edu.cn 属性”对话框，选择“起始授权机构（SOA）”标签，如图 7.35 所示。在此对话框中可以设置以下这些值。

- 序列号：当执行区域传输时，首先检查序列号，只有当主服务器的序列号比辅助服务器的序列号大的时候（表示辅助服务器中的数据已过时）复制操作才会执行。
- 主服务器：此区域的主服务器的完全合格域名。
- 负责人：此区域的负责人的电子邮箱地址。
- 刷新间隔：设置辅助服务器隔多长时间需要检查其数据，执行区域传输。
- 重试间隔：当在刷新间隔到期时辅助服务器无法与主服务器通信，需等待多久再重试。
- 过期间隔：如果辅助服务器一直无法与主服务器建立通信，在此时间间隔后辅助服务器不再执行查询服务，因为其包含的数据可能是错误的。
- 最小 TTL：服务器查询到的数据在缓存中的保存时间。

步骤 12：DNS服务器的维护

1）设置 DNS 服务器的动态更新

在 Windows Server 2003 中可以利用动态更新的方式，当 DHCP 主机 IP 地址发生变化时，会在 DNS 服务器中自动更新，这样可以减轻管理员的负荷。具体设置如下：

① 首先用户需要对 DHCP 服务器的属性进行设置，右击“DHCP 服务器”，在弹出的菜单中选择“属性”选项，单击“DNS”标签，如图 7.36 所示，在其中选中“根据下面的设置启用 DNS 动态更新”和“在租约被删除时丢弃 A 和 PTR 记录”选项。

② 在 DNS 控制台中展开正向查找区域，选择区域 xpc.edu.cn，执行“操作→属性”命令，在“常规”标签中的“动态更新”下拉列表中选择“非安全”选项，单击“确定”按钮。如图 7.37 所示。

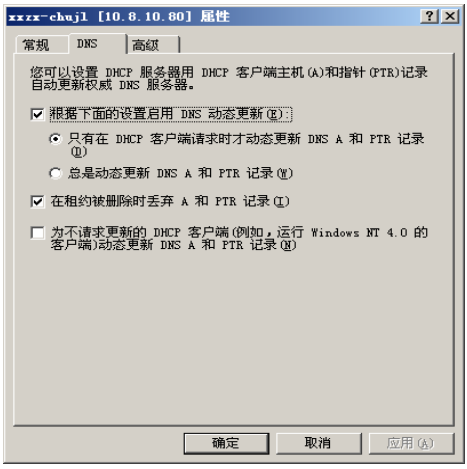

图 7.36 “作用域→DNS”对话框

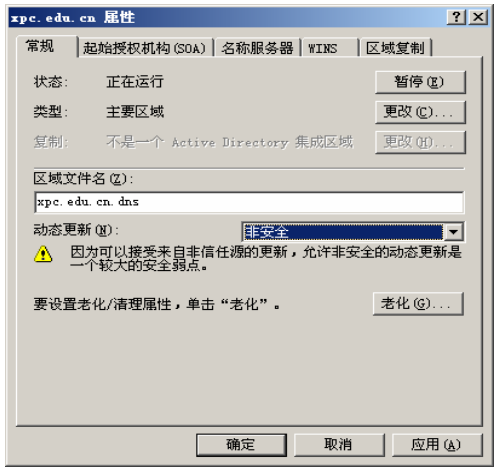

图 7.37 “xpc.edu.cn 属性”对话框

③ 展开反向查找区域，选择“反向区域”选项，单击“属性”选项，并在“常规”标签中的“动态更新”下拉列表中选择“非安全”选项。

这样在客户信息改变时，它在 DNS 服务器中的信息也会自动更新。

2）指定根域服务器（root 服务器）

当 DNS 服务器要向外界的 DNS 服务器查询所需的数据时，在没有指定转发器的情况下，它先向位于根域的服务器进行查询。然而，DNS 服务器是通过缓存文件来知道根域的服务器。缓存文件在安装 DNS 服务器时就已经存放在\winnt\system32\dns 文件夹内，其文件名为 cache.dns。cache.dns 是一个文本文件，可以用文本编辑器进行编辑。

如果一个局域网没有接入 Internet，这时内部的 DNS 服务器就不需要向外界查询主机的数据，这时需要修改局域网根域的 DNS 服务器数据，将其改为局域网内部最上层的 DNS 服务器的数据。如果在根域内新建或删除 DNS 服务器，则缓存文件的数据就需要进行修改。修改时建议不要直接用编辑器进行修改，而采用如下的方法进行修改。

执行“开始→程序→管理工具→DNS”命令，右击 DNS 服务器名称，如 xxzx-chujl，在弹出的菜单中选择“属性”选项，再单击“根提示”标签，弹出“DNS 根目录属性”对话框，如图 7.38 所示。在该对话框的列表中列出了根域中已有的 DNS 服务器及其 IP 地址，用户可以单击“添加”按钮添加新的 DNS 服务器。

3）设置转发器

当 DNS 服务器收到自己无法解析的 DNS 请求时，默认将查询 Internet 的根域 DNS 服务器，而全球仅有的十几台根 DNS 服务器都在国外，因此会造成客户较长时间的等待。这时可以在 DNS 服务器上配置“转发器”，把自己无法解析的查询转发到邻近的其他 DNS 服务器上。

单击图 7.38 中的“转发器”标签，弹出如图 7.39 所示的“转发器属性”对话框。在该对话框中选中“启用转发器”选项，输入作为转发器的 DNS 服务器 IP 地址，如 202.99.160.68，单击“添加”按钮，将 IP 地址为 202.99.160.68 的 DNS 服务器作为该 DNS 服务器的转发器。

用户可以单击“添加”按钮添加新的 DNS 服务器。

4）启用日志记录功能

单击图 7.39 中的“日志”标签，弹出如图 7.40 所示的“日志属性”对话框。在该对话

框中选择需要的日志记录选项。

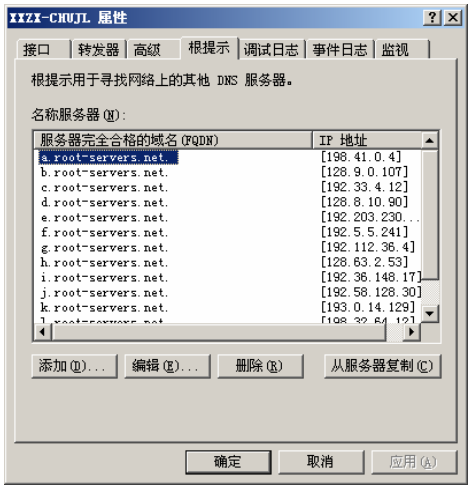

图 7.38 “根提示”对话框

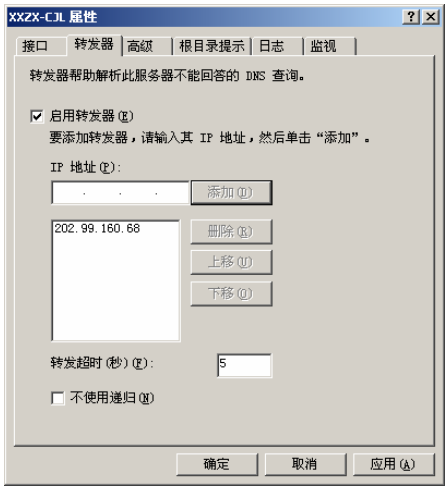

图 7.39 “转发器属性”对话框

5）配置多宿主 DNS 服务器

所谓多宿主 DNS 服务器，是指安装 DNS 服务器的计算机拥有多个 IP 地址。在默认情况下，DNS 服务器侦听所在计算机上所有的 IP 地址，接受发送至其默认服务端口的所有客户机请求。管理员可以对特定的 IP 地址闲置 DNS 服务，使 DNS 服务仅侦听和应答发送至指定的 IP 地址的 DNS 请求。单击图 7.39 中的“接口”标签，弹出如图 7.41 所示的“接口属性”对话框。

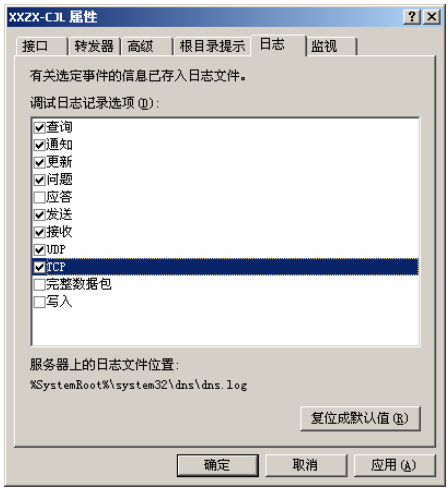

图 7.40 “日志属性”对话框

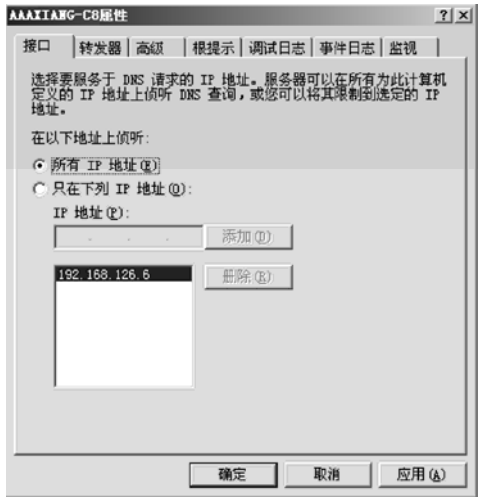

图 7.41 “接口属性”对话框

步骤 13：测试配置的DNS服务器

从步骤 3 到步骤 12 都是在安装 Windows Server 2003 系统的计算机上配置 DNS 的步骤，下面在 DNS 客户端 PCA、PCB 的计算机对刚才配置的 DNS 进行测试。

1）配置测试主机

在成功安装 DNS 服务器后，就可以在 DNS 客户机启用 DNS 服务。在 PCA 和 PCB 上分别设置，以在 PCA 上设置为例。打开“网络和拨号连接”对话框，双击“本地连接”选项，

单击“属性”按钮，选择“Internet 协议（TCP/IP）”选项，然后单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，如图 7.42 所示。如果在 DHCP 服务中设置了 DNS 的信息，则在对话框中选择“自动获得 DNS 服务器地址”选项，并分别在首选 DNS 服务器和备用 DNS 服务器中填写主 DNS 服务器和辅助 DNS 服务器的 IP 地址。

2）DNS 正向解析测试

选择“开始→运行”命令，输入“ipconfig/all”，查看 DNS 服务器的配置情况，确认已配置了 DNS 服务器。

在 IE 地址栏中输入 www.xpc.edu.cn、mail.xpc.edu.cn、www.dzx.xtvt.edu.cn，观察域名服务器解析是否正确，能否访问因特网。

在 MS－DOS 环境下，利用 ping 命令解析 www.sina.com.cn、www.yahoo.com.cn、www.sohu.com 等主机域名的 IP 地址，如图 7.43 所示。

3）DNS 反向解析测试

反向解析测试主要是测试 DNS 服务器是否能够提供名称解析功能。在命令状态下输入 ping-a 192.168.11.250，以检测 DNS 服务器是否能够将 IP 地址解析成主机名。

4）使用 nslookup 命令测试 DNS 服务器

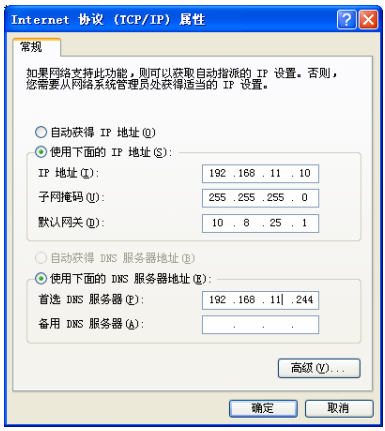

图 7.42　Internet 协议（TCP/IP）属性

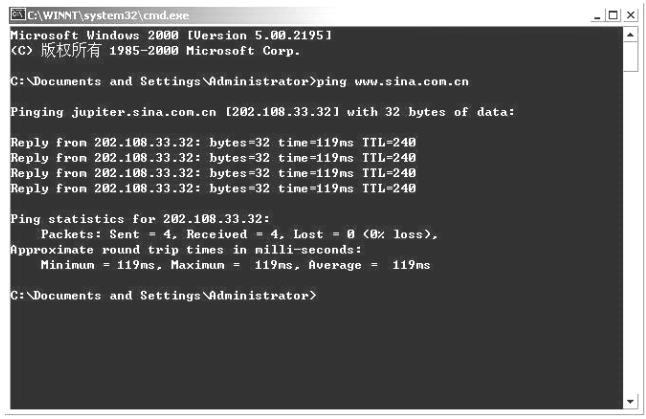

图 7.43　使用 ping 命令检测 DNS 配置

nslookup 是一个有用的实用程序，它通过向 DNS 服务器查询信息，能够诊断解决像主机名称解析这样的 DNS 问题。启动 nslookup 时，显示本地主机配置的 DNS 服务器主机名和 IP 地址。WindowsNT/2000/XP 系统都提供该工具；Windows95/98 系统不提供该工具。

（1）使用 nslookup。在命令提示符下，输入“nslookup”，进入 nslookup 交互模式，出现“>”提示符，这时输入域名或 IP 地址等资料，按 Enter 键可得到相关信息。

（2）nslookup 中的其他常用命令及说明。所有的命令需在“>”提示符后面输入，常用命令有：

- help：显示有关帮助信息。
- exit：退出 nslookup 程序。
- server IP：将默认的服务器更改到指定的 DNS 域。IP 为指定 DNS 服务器的 IP 地址。
- set q=A：由域名查询 IP 地址。为默认设定值。
- set q=CNAME：查询别名的规范名称。

➢ set q=ANY：查询所有数据类型。

➢ set q=PTR：如果查询的是 IP 地址，则结果为计算机名；否则为指向其他信息的指针。

➢ set q=MX：查询邮件交换器。

➢ set q=NS：查询用于命名区域的 DNS 名称服务器。

（3）nslookup 使用举例。假设 DNS 服务器为 192.168.11.200，域为 xpc.edu.cn，在客户端启动 nslookup，输入下面的命令：

```
> server 192.168.11.250              \\将默认服务器设为 192.168.11.250
Default Server: host.xpc.edu.cn      \\返回的信息
Address: 192.168.11.250
> set q=A                            \\正向域名查询
> www.xpc.edu.cn                     \\查询 www.xpc.edu.cn
Server: host.xpc.edu.cn
Address:192.168.11.250
Non-authoritative answer:
Name: www.xpc.edu.cn
Address: 192.168.11.250              \\查询到的结果
```

5）查看主机的域名高速缓存区

为了提高主机的解析效率，主机常常采用高速缓冲区来存储检索过的域名与其 IP 地址的映射关系。UNIX、Linux、Windows Server 2003 等操作系统都提供命令，允许用户查看域名高速缓冲区中的内容。在 Windows Server 2003 中，ipconfig/displaydns 命令可以将高速缓冲区中的域名与其 IP 地址映射关系显示在屏幕上，包括域名、类型、TTL、IP 地址等。如图 7.44 所示。如果需要清除主机高速缓冲区中的内容，可以使用 ipconfig/flushdns 命令。

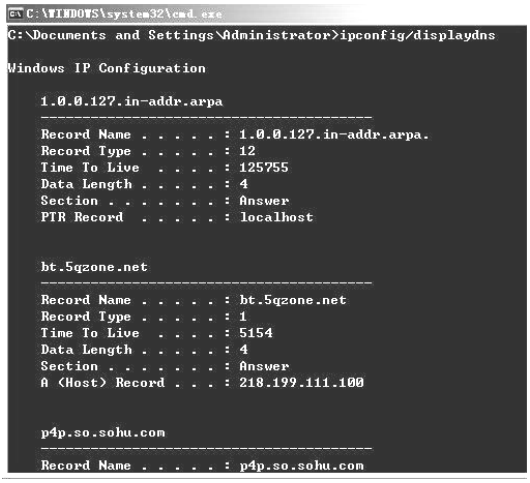

图 7.44　ipconfig/displaydns 查看高速缓冲区

步骤 14：备份与还原DNS服务

备份与还原 DNS 服务主要分两步进行，一是备份 DNS 注册表，二是备份 DNS 配置文件。

（1）备份 DNS 配置文件。备份 DNS 配置文件是将 DNS 域名数据备份出来。DNS 域名数据信息文件位于 c:\windows\system32\dns 目录下，可以直接把该目录下后缀为.dns 的所有文件都复制到备份目录下。这些.dns 文件中存储着域名解析时所使用的域名数据信息。

（2）还原 DNS 服务。

① 当区域里的DNS服务器发生故障，重新建立一台Windows Server 2003服务器，并与所要替代的DNS服务器名字相同，设置相同的DNS后缀和IP地址。

② 在新系统中安装并启动 DNS 服务。

③ 把前面备份出来的＊.dns 文件复制到新系统的\windows\system32\dns 文件夹中。

④ 停用 DNS 服务。

⑤ 把备份的 dns-bak.reg 和 dns-bakserver.reg 导入注册表中。

⑥ 重新启动 DNS 服务。

7.5 扩展知识及任务训练

7.5.1 中文域名系统

1．中文域名概念

简单地说，中文域名是现有域名体系的最新发展，是互联网的基础服务。中文域名是含有中文文字的域名。经原信息产业部批准，我国域名注册管理机构中国互联网络信息中心（CNNIC）于 2000 年推出了中文域名系统。

中文域名和 CN 域名属于域名体系，中文域名是符合国际标准的一种域名体系，使用上和英文域名近似，作为域名的一种，可以通过 DNS 解析，支持虚拟主机、电子邮件等服务。

通用网址是一种新兴的网络名称访问技术，是通过建立通用网址与网站地址 URL 的对应关系，实现浏览器访问的一种便捷方式，是基于 DNS 之上的一种访问技术。

注册中文域名有以下优点：

① 对于中国人而言，使用方便，便于记忆。

② 中文域名资源丰富，可以获得满意的域名。注册一个中文.中国域名，将自动获得中文.cn 这样的域名。

③ 注册一个简体中文域名，自动获赠繁体中文域名，域名注册手续简便、快捷。

④ 显著的标志作用，体现自身的价值和定位。

⑤ 全中文服务，保障用户知情权。

⑥ 适用中国法律，全面保障用户利益。

⑦ 保障国家域名系统的安全。

2003 年 5 月，CNNIC 根据国际标准，正式推出了符合国际标准的中文域名系统，并在网站上发布，供广大用户免费下载使用。

2．中文域名结构

中文域名系统原则上遵照国际惯例，采用树状分级结构，系统的根不被命名，其下一级称为“中文顶级域”（CTLD），顶级域一般由“地理域”组成，二级域为“类别/行业/市地域”，三级域为“名称/字号”。格式为：

地理域.类别/行业/市地域.名称/字号

国家标准最主要特征是中文域名的结构符合中文语序，例如，北京航空航天大学的中文域名是：北京.教育.北京航空航天大学。其中，北京航空航天大学域下的子域名由其自行定义，例如，北京.教育.北京航空航天大学.经济管理学院 MBA。

3．中文域名类型

根据原信息产业部《关于中国互联网络域名体系的公告》，中文域名分为以下 4 种类型：中文.cn、中文.中国、中文.公司和中文.网络。即注册的中文域名至少需要含有一个中文文字。可以选择中文、英文字母（A-Z，a-z，大小写等价）、数字（0～9）或符号（-）命名中文域名，但最多不超过 20 个字符。例如：

- 中国互联网络信息中心.中国
- 中国互联网络信息中心.cn
- 中国互联网络信息中心.公司
- 中国互联网络信息中心.网络

4．中文域名的使用

在使用中文域名时，用户只需在 IE 浏览器地址栏中直接输入中文域名，如“http://北京大学.cn”，即可访问相应网站。如果用户觉得输入 http 的引导符比较麻烦，并且不愿意切换输入法，希望用“。”来代替“.”，那么只要到中国互联网络信息中心网站安装中文域名的软件就可以实现，例如，输入“北京大学。cn”即可访问北京大学的网站。

7.5.2 动态DNS（域名解析）服务

动态 DNS（域名解析）服务，是可以将固定的互联网域名和动态（非固定）IP 地址实时对应（解析）的服务。相对于传统的静态 DNS 而言，它可以将一个固定的域名解析到一个动态的 IP 地址，简单地说，无论用户何时上网、以何种方式上网、得到一个什么样的 IP 地址、IP 地址是否会变化，他都能保证通过一个固定的域名就能访问到用户的计算机。

动态域名的功能是实现固定域名到动态 IP 地址之间的解析。用户每次上网得到新的 IP 地址之后，安装在用户计算机里的动态域名软件就会把这个 IP 地址发送到动态域名解析服务器，更新域名解析数据库。因特网上的其他人要访问这个域名的时候，动态域名解析服务器会返回正确的 IP 地址。

习　题

一、填空题

1．DNS 又称_____。在 Internet 上访问某个网站是通过 IP 地址寻址来解决的，但 IP 地址是一串数字，比较难记，于是产生了_____和_____的相互翻译。

2．DNS 服务器工作在 OSI 参考模型的_____层。

3．现在顶级域名有_____ 、_____、_____三大类。

4．在我国将二级域名划分为_____和 _____两大类。

5．域名服务器是整个域名系统的核心，因特网上的域名服务器有_____、_____、_____3 种类型。

6．反向型查询是依据 DNS 客户端提供的_____来查询它的_____。

7．为了提高解析速度，域名解析服务提供了_____和_____两方面的优化。

8．域名解析使用_____协议，其 UDP 端口号为_____。提出 DNS 解析请求的主机与域名服务器之间采用_____模式工作。

9．当 DNS 服务器要向外界的 DNS 服务器查询所需的数据时，在没有指定转发器的情况下，它先向位于_____的服务器进行查询。

10．中文域名系统原则上遵照国际惯例，采用树状分级结构，系统的根不被命名，其下一级称为“中文顶级域”（CTLD），顶级域一般由“地理域”组成，二级域为“类别/行业/市地域”，三级域为“名称/字号”。格式为_____。

11．目前有_____、_____、_____、_____4 种类型的中文域名。

12．在 Windows 命令窗口输入_____命令来查看 DNS 服务器的 IP。

13．DNS 服务器（DNS 服务器有时也扮演 DNS 客户端的角色）向另一台 DNS 服务器查询 IP 地址时，可以有 3 种查询方式：_____、_____ 和_____。

14．若希望 IP 地址映射成域名，则应选择_____。

15．一个 IP 地址可以对应_____（单个/多个）域名；一个域名可以对应_____（单个/多个）IP 地址。

二、选择题

1．DNS 服务器和客户机设置完毕后，有 3 个命令可以测试其设置是否正确，下面（　　）不是其中之一。

A．PING　　B．LOGIN　　C．IPCONFIG　　D．NSLOOKUP

2．DNS 的作用是（　　）。

A．用来将端口翻译成 IP 地址

B．用来将域名翻译成 IP 地址

C．用来将 IP 地址翻译成硬件地址

D．用来将 MAC 翻译成 IP 地址

3．在 www.tsinghua.edu.cn 这个完全合格域名里，（　　）是主机名。

A．edu. cn　　B．tsinghua　　C．tsinghua. edu. cn　　D．www

4．将域名地址转换为 IP 地址的协议是（　　）。

A．DNS　　B. ARP　　C．RARP　　D．ICMP

5．域名服务器上存放有 Internet 主机的（　　）。

A．域名　　B．IP 地址

C．域名和 IP 地址　　D．E-mail 地址

6．为了实现域名解析，客户机（　　）。

A．必须知道授权域名服务器的 IP 地址

B．必须知道本地域名服务器的 IP 地址

C．必须知道授权域名服务器的 IP 地址

D．知道互联网上任意一个域名服务器的 IP 地址即可

7．DNS 区域有 3 种类型，下面哪一个不是？（　　）

A．标准辅助区域　　B．逆向解析区域

C．Active Directory 集成区域　　D．标准主要区域

8．表示主机记录的资源记录简写是（　　）。

A．A　　B．MX　　C．CNAME　　D．PTR

9．表示别名的资源记录是（　　）。

A．SOA　　B．MX　　C．CNAME　　D．PTR

10．DNS 域名解析体系中，为了便于管理，DNS 服务器不用解析本区域的所有子域的主机名，而是由子域 DNS 服务器进行解析。在父域 DNS 服务器上通过（　　）操作，将域名解析请求转发给子域的 DNS 服务器要求解析。

A．委派　　B．转发　　C．递归　　D．轮询

11．DNS 域名解析体系中，当某个 DNS 服务器不用解析某个域名请求，且该域名不属于它管理的区域时，应该通过（　　）操作向其他 DNS 服务器申请解析。

A．委派　　B．转发　　C．搜索　　D．轮询

三、思考题

1．域名结构如何划分？

2．中文域名是如何划分的？

3．在因特网上，域名服务器的作用是什么？有哪几种域名服务器？

4．分析 DNS 服务名称解析原理，以及反向型查询原理。

5．在 DNS 事件日志中能找到什么信息？

6．简述域名的解析过程。

7．分析中文域名的结构。

8．中文域名有哪几种类型？

9．怎样在客户机上配置 DNS 服务器？

10．别名有何作用？如何使用？

四、实训题

在 PCA 计算机上设置 DNS 服务器，建立标准的正向查找区域（lianxi.com）和反向查找区域（192.168.1），并在正向区域添加 Web 服务器（www，A 记录，192.168.1.100），FTP 服务器（ftp，A 记录，192.168.1.110）和 Mail 服务器（mail，A 和 MX 记录，192.168.1.111）。

在 PCB（安装 Windows XP 系统）上进行客户端验证，包括使用 ping、nslookup 等。

项目 8　利用DHCP自动分配IP地址

在使用 TCP/IP 的网络中，每一台计算机都必须有一个唯一的 IP 地址，并且通过此 IP 地址来与网络中的其他主机通信。IP 地址的设置可以使用以下两种方法：静态分配和自动获取。

1．手工静态设置

手工静态设置是一种手工输入方式，它要求网络管理人员根据本网络的 IP 地址规划，为每一个接入网络的客户端分配一个固定的 IP 地址，并手工配置网关、DNS 服务器等相关的参数。

2．自动向DHCP服务器索取

当网络中的计算机数量较多时，可以使用动态的 IP 地址，此时不必输入固定的 IP 地址，而由 DHCP 服务器自动分配，这样可以减少手工设置所造成的错误，减轻管理上的负担。

8.1　任务 1：基于Windows Server 2003 的DHCP 实现和应用

8.1.1　任务内容

1．任务目的

通过安装和配置 DHCP 服务器，理解 DHCP 的工作原理，掌握使用 DHCP 进行网络管理的基本方法。DHCP 是网络服务的一种，其他网络服务的安装配置与 DHCP 有许多相同之处，通过实训，理解网络服务的概念，掌握在 Windows Server 2003 操作系统中安装配置网络服务的一般性方法。

2．实训任务

某公司组建单位内部的局域网，随着计算机数量的增加，网络管理员在客户机的 TCP/IP 维护上花费了不少的时间，首先在连入单位内部网络时需要分配 IP 地址，另外有些客户在计算机重新安装操作系统后经常询问自己计算机的 IP 地址等信息，在这种情况下，需要在局域网内部安装并配置一台 DHCP 服务器，为公司内除服务器以外的所有计算机自动配置 IP 地址、子网掩码、默认网关、DNS 服务器地址等网络参数。

3．任务目标

① 了解 TCP/IP 网络中 IP 地址的分配方式和特点；
② 理解 DHCP 的基本概念和运行原理；
③ 学会在 Windows Server 2003 系统中 DHCP 服务器的安装和配置方法；
④ 学会 DHCP 作用域的配置方法；
⑤ 学会 DHCP 客户端的设置方法。

8.1.2 相关知识

1．DHCP的概念

DHCP 是 Dynamic Host Configuration Protocol 的缩写，中文译为动态主机配置协议，它是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。

在使用 DHCP 服务时，整个网络至少有一台服务器上安装了 DHCP 服务，其他要使用 DHCP 功能的客户机必须设置为利用 DHCP 获得 IP 地址。客户机在向服务器请求一个 IP 地址时，如果还有 IP 地址没有使用，则在数据库中登记该 IP 地址已被该客户机使用，然后回应这个 IP 地址以及相关的选项给客户机。图 8.1 是一个支持 DHCP 的网络实例。

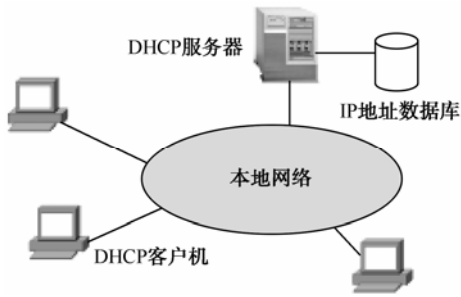

图 8.1　DHCP 服务示意图

2．DHCP的基本术语

（1）作用域：作用域是用于网络的 IP 地址的完整连续范围。作用域通常定义提供 DHCP 服务的网络上的单独物理子网。作用域还为服务器提供管理 IP 地址的分配和指派及与网上客户相关的任何配置参数的主要方法。

（2）超级作用域：超级作用域是可用于支持相同物理子网上多个逻辑 IP 子网的作用域的管理性分组。

（3）排除范围：排除范围是作用域内从 DHCP 服务中排除的有限 IP 地址序列。排除范围确保在这些范围中的任何地址都不是由网络上的服务器提供给 DHCP 客户机的。

（4）地址池：在定义 DHCP 作用域并应用排除范围之后，剩余的地址在作用域内形成可用地址。

（5）租约：租约是客户机可使用指派的 IP 地址期间 DHCP 服务器指定的时间长度。租用给客户时，租约是活动的。

（6）租期：租期是指 DHCP 客户端从 DHCP 服务器获得完整的 TCP/IP 配置后，对该 TCP/IP 配置的使用时间。

（7）保留：使用保留创建通过 DHCP 服务器的永久地址租约指派。

（8）选项类型：是 DHCP 服务器在向 DHCP 客户机提供租约服务时指派的其他客户机配置参数。例如，某些公用选项包含用于默认网关（路由器）、WINS 服务器和 DNS 服务器的 IP 地址。

（9）选项类别：是一种可供服务器进一步管理提供给客户的选项类型的方式。当选项类别添加到服务器时，可为该类别的客户机提供用于其配置的类别特定选项类型。

3．DHCP的工作原理

1）DHCP 的工作过程

当作为 DHCP 客户端的计算机第一次启动时，它通过一系列的步骤获得其 TCP/IP 配置信息，并得到 IP 地址的租期。DHCP 客户端从 DHCP 服务器上获得完整的 TCP/IP 配置需要经过以下几个过程，如图 8.2 所示。

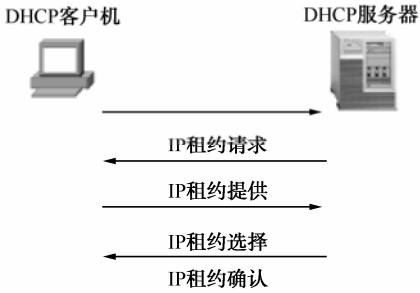

图 8.2　DHCP 工作过程

（1）DHCP 发现：DHCP 工作过程的第一步是 DHCP 发现（DHCP Discover），该过程也称之为 IP 发现。以下几种情况需要进行 DHCP 发现。

- 当客户端第一次以 DHCP 客户端方式使用 TCP/IP 协议栈时，即第一次向 DHCP 服务器请求 TCP/IP 配置时；
- 客户端从使用固定 IP 地址转向使用 DHCP 动态分配 IP 地址时；
- 该 DHCP 客户端所租用的 IP 地址已被 DHCP 服务器收回，并已提供给其他的 DHCP 客户端使用时。

当 DHCP 客户端发出 TCP/IP 配置请求时，DHCP 客户端既不知道自己的 IP 地址，也不知道服务器的 IP 地址。DHCP 客户端便将 0.0.0.0 作为自己的 IP 地址，将 255.255.255.255 作为服务器的地址，然后在 UDP（用户数据协议）的 67 或 68 端口广播发送一个 DHCP 发现信息。该发现信息含有 DHCP 客户端网卡的 MAC 地址和计算机的 NetBIOS 名称。

当第一个 DHCP 发现信息发送出去后，DHCP 客户端将等待 1 秒钟。在此期间，如果没有 DHCP 服务器做出响应，DHCP 客户端将分别在第 9 秒、第 13 秒和第 16 秒时重复发送一次 DHCP 发现信息。如果还没有得到 DHCP 服务器的应答，DHCP 客户端将每隔 5 分钟广播一次发现信息，直到得到一个应答为止。如果网络中没有可用的 DHCP 服务器，基于 TCP/IP 协议栈的通信将无法实现。这时，DHCP 客户端如果是 Windows Server 2000 用户，就自动选一个自认为没有被使用的 IP 地址（该 IP 地址可从 169.256.x.y 地址段中选取）使用。尽管此时客户端已分配了一个静态 IP 地址（但还没有重新启动计算机），DHCP 客户端还要每隔 5 分钟发送一次 DHCP 发现信息。如果这时有 DHCP 服务器响应，DHCP 客户端将从 DHCP 服务器获得 IP 地址及其配置，并以 DHCP 方式工作。

（2）DHCP 提供：DHCP 工作的第二步是 DHCP 提供（DHCP Offer），是指当网络中的任何一个 DHCP 服务器（同一个网络中可能存在多个 DHCP 服务器）在收到 DHCP 客户端的 DHCP 发现信息后，该 DHCP 服务器若能够提供 IP 地址，就从该 DHCP 服务器的 IP 地址池中选取一个没有出租的 IP 地址，然后利用广播方式提供给 DHCP 客户端。在还没有将该 IP 地址正式租用给 DHCP 客户端之前，这个 IP 地址会暂时保留起来，以免再分配给其他的 DHCP 客户端。

如果网络中有多台 DHCP 服务器，且这些 DHCP 服务器都收到了 DHCP 客户端的 DHCP 发现信息，同时这些 DHCP 服务器都广播一个应答信息给该 DHCP 客户端时，则 DHCP 客户端将从收到应答信息的第一台 DHCP 服务器中获得 IP 地址及其配置。

提供应答信息是 DHCP 服务器发给 DHCP 客户端的第一个响应，它包含了 IP 地址、子网掩码、租用期（以小时为单位）和提供响应的 DHCP 服务器的 IP 地址。

（3）DHCP 请求：DHCP 工作的第三步是 DHCP 请求（DHCP Request），一旦 DHCP 客户端收到第一个由 DHCP 服务器提供的应答信息，就进入此过程。当 DHCP 客户端收到第一个 DHCP 服务器响应信息后，就以广播的方式发送一个 DHCP 请求信息给网络中所有的 DHCP 服务器。在 DHCP 请求信息中包含所选择的 DHCP 服务器的 IP 地址。

（4）DHCP 应答：DHCP 工作的最后一步是 DHCP 应答（DHCP ACK）。一旦被选择的 DHCP 服务器接收到 DHCP 客户端的 DHCP 请求信息，就将已保留的这个 IP 地址标志为已

租用，然后也以广播方式发送一个 DHCP 应答信息给 DHCP 客户端。该 DHCP 客户端在接收 DHCP 应答信息后，就完成了获得 IP 地址的过程，便开始利用这个已租到的 IP 地址与网络中的其他计算机进行通信。

2）IP 地址的租用和续租

当一台 DHCP 客户端租到一个 IP 地址后，该 IP 地址不可能长期被它占用，它会有一个使用期，即租期。当租期已到时需要续租该怎么办呢？当 DHCP 客户端的 IP 地址使用时间达到租期的一半时，它就向 DHCP 服务器发送一个新的 DHCP 请求（相当于新租用一个 IP 地址的第三步），若服务器在接收到该信息后并没有理由拒绝该请求，便回送一个 DHCP 应答信息（相当于新租用一个 IP 地址时的最后一步），当 DHCP 客户端收到该应答信息后，就重新开始一个租用周期。此过程就像对一个合同的续约，只是续约时间必须要在合同期的一半时签订。

在进行 IP 地址的续租过程中有以下两种特例。

（1）DHCP 客户端重新启动时：不管 IP 地址的租期有没有到期，当每一次启动 DHCP 客户端时，它都会自动利用广播的方式，给网络中所有的 DHCP 服务器发送一个 DHCP 请求信息，以便请求该 DHCP 客户端继续使用原来的 IP 地址及其配置。如果此时没有 DHCP 服务器对此请求应答，而原来 DHCP 客户端的租期还没有到期，那么 DHCP 客户端还会继续使用该 IP 地址。

（2）IP 地址的租期超过一半时：当 IP 地址的租期到达一半的时间时，DHCP 客户端会向 DHCP 服务器发送（非广播方式）一个 DHCP 请求信息，以便续租该 IP 地址。当续租成功后，DHCP 客户端将开始一个新的租用周期，而当续租失败后，DHCP 客户端仍然可以继续使用原来的 IP 地址及其配置，但是该 DHCP 客户端将在租期到达 87.8%的时候再次利用广播方式发送一个 DHCP 请求信息，以便找到一台可以继续提供租期的 DHCP 服务器。如果续租仍然失败，则该 DHCP 客户端会立即放弃其正在使用的 IP 地址，以便重新向 DHCP 服务器获得一个新的 IP 地址（需要进行完整的 4 个步骤）。

在以上的续租过程中，如果续租成功，DHCP 服务器会给该 DHCP 客户端发送一个 DHCP ACK 信息，DHCP 客户端在收到该 DHCP ACK 信息后进入一个 IP 地址租用周期；当续租失败时，DHCP 服务器将会给该 DHCP 客户端发送一个 DHCP NACK 信息，DHCP 客户端在收到该信息后，说明该 IP 地址已经无效或被其他的 DHCP 客户端使用。

4．DHCP服务器分配IP地址的方式

当 DHCP 客户端启动时，它会向 DHCP 服务器发出信息，要求 DHCP 服务器提供 IP 地址，而 DHCP 服务器在接收到 DHCP 客户端的请求后，则根据 DHCP 服务器端的设置，决定如何提供 IP 地址给客户端，通常有以下两种方式：

（1）永久租用：当 DHCP 服务器向 DHCP 客户端提供一个 IP 地址后，这个 IP 地址就永远归这个 DHCP 客户端使用。当网络中有足够的 IP 地址可供给客户端使用时，就可以采用这种方式给客户端自动分配 IP 地址。

（2）限定租用：当 DHCP 客户端从 DHCP 服务器获得 IP 地址后，DHCP 客户端可以使用这个 IP 地址一段时间。但当租约到期时，如果客户端没有重新租约，则 DHCP 服务器会收回这个 IP 地址，并将该 IP 地址提供给其他 DHCP 客户端使用。当网络中的 IP 地址不够用时，可用这种方式给客户端自动分配 IP 地址。

8.1.3 方案设计及准备

在单位内架设的 DHCP 服务器的操作系统可以是 Windows Server 2003，也可以是 Linux 系统。在本测试环境中，DHCP 服务器操作系统采用 Windows Server 2003。

1．设计

在一个私有 192.168.11.0 的网络上，子网掩码为 255.255.255.0，IP 地址规划为：

① DHCP 服务器 IP 地址为 192.168.11.240，名称为子网 1，可分配的 IP 地址为 192.168.11.2～192.168.11.254；

② 默认网关地址为 192.168.11.1；

③ 固定地址的服务器地址为 192.168.11.240～192.168.11.254，保留用于 DNS、Web、FTP、WSUS 等服务器；

④ DNS 服务器地址为 202.99.160.68。

根据以上要求，本项目实施的网络拓扑结构如图 8.3 所示。

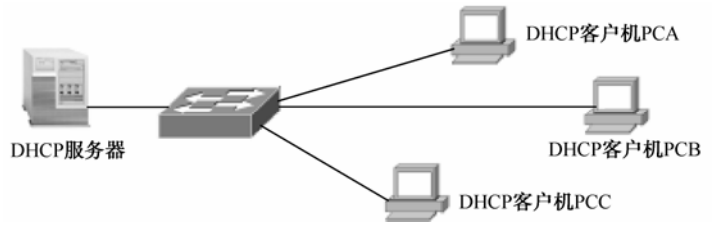

图 8.3 DHCP 服务网络拓扑图

2．设备清单

为了搭建如图 8.3 所示的网络环境，需要的设备和连线主要包括：

① 安装 Windows Server 2003 系统的 PC 计算机 1 台；

② 测试用计算机 3 台（Windows XP 系统）；

③ 直通线 4 条；

④ 交换机 1 台。

8.1.4 项目实施

通常认为每 10 000 个客户需要 2 台 DHCP 服务器，一台作为主服务器，另一台作为备份服务器。对于一台 DHCP 服务器没有客户数的限制，在实际中受用户所使用的 IP 地址所在的地址分类及服务器配置（如磁盘的容量、CPU 的处理速度等）的限制。

步骤 1：硬件连接

按照图 8.3 所示，将 4 台计算机通过直通线连接到交换机上，搭建本实训项目网络环境。

步骤 2：进行TCP/IP设置

因为要配置 DHCP 服务器，客户机通过 DHCP 自动获得 IP 地址等信息，所以客户机不需要配置 IP 地址。而充当 DHCP 服务器的计算机需要设置 IP 地址，设置为 192.168.11.240，子网掩码为 255.255.255.0，网关为 192.168.11.1。

步骤 3：安装DHCP服务器

在 Windows Server 2003 系统中默认没有安装 DHCP 服务，需要另外单独安装。DHCP 服务安装步骤如下。

（1）选择“开始→设置→控制面板→添加/删除程序→添加/删除 Windows 组件”命令，弹出“Windows 组件”对话框，选中“网络服务”复选框，单击“详细信息”按钮，在弹出的“网络服务”对话框中，选中“动态主机配置协议”复选框，如图 8.4 所示，然后单击“确定”按钮。

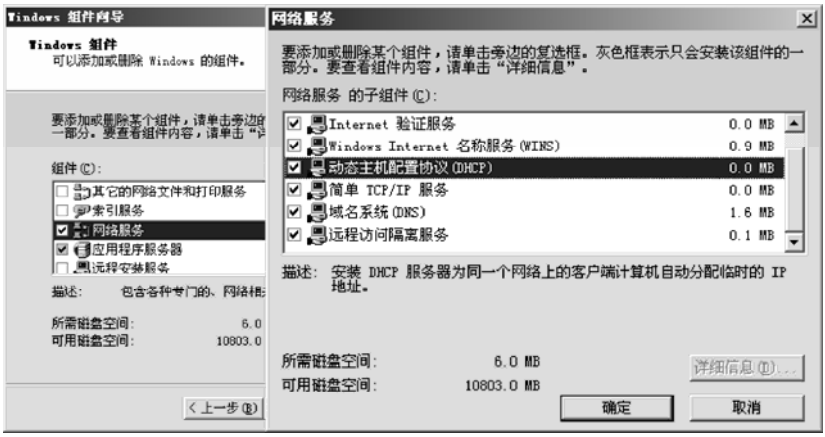

图 8.4 “DHCP 服务”安装过程

（2）单击“下一步”按钮，Windows 组件向导会完成 DHCP 服务的安装，并从 Windows Server 2003 安装光盘中复制所需文件。

（3）重新启动计算机，完成 DHCP 服务安装。安装完毕后在管理工具中多了一个“DHCP”选项。

步骤 4：DHCP服务器的授权

在安装 DHCP 服务后，用户必须首先添加一个授权的 DHCP 服务器。

（1）以管理员身份登录。

（2）选择“开始→程序→管理工具→DHCP”命令，进入“DHCP”控制台窗口。

（3）右击“DHCP”控制台窗口左边栏的要授权的 DHCP 服务器，本例中为 xxzx-chujl.xpc.edu.cn，从弹出的菜单中选择“授权”选项，完成授权。如图 8.5 所示。再右击要授权的 DHCP 服务器 xzx-chujl.xpc.edu.cn［192.168.11.240］，可以看见在弹出的菜单中“授权”选项已经变为“撤销授权”选项。

在 Windows Server 2003 的网络中，如果 DHCP 服务器没有授权，是不能为网络中的客户端分配 IP 地址的。没有授权的 DHCP 服务器前面的“计算机图标”有一个红色的“箭头”，经过授权的 DHCP 服务器前面的“计算机图标”有一个绿色的“箭头”。

（4）若要解除授权，只要右击该服务器，选择“撤销授权”选项即可。

（5）右击“DHCP”，从弹出的菜单中选择“管理授权的服务器”选项，弹出“管理授权的服务器”对话框，如图 8.6 所示，在此可以授权和撤销授权。

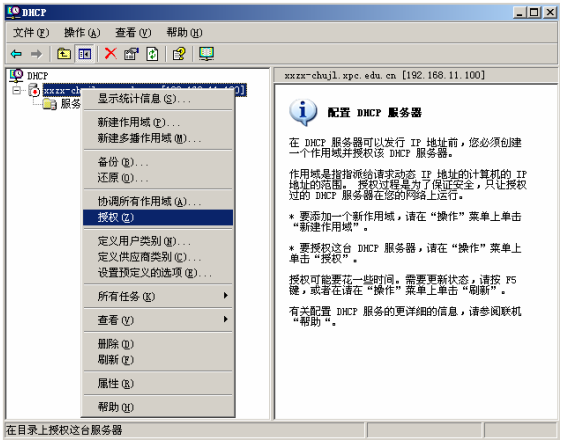

图 8.5　授权“DHCP 服务器”

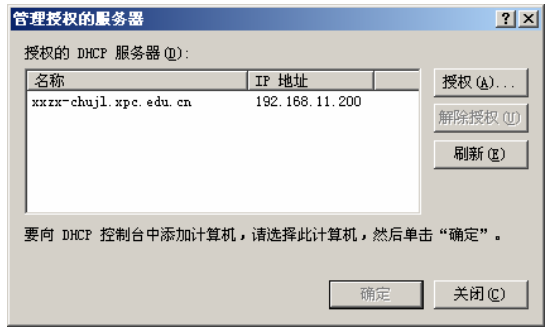

图 8.6　“管理授权的服务器”对话框

在进行 DHCP 授权时应注意如下事项。

（1）Windows Server 2003 域中的所有 DHCP 服务器都必须被授权。未经授权的 DHCP 服务器并不会提供 DHCP 服务，也不会将 IP 地址租给 DHCP 客户端。

（2）只有 Enterprise Admin 组内的成员才有权执行授权的操作。

（3）已被授权的 DHCP 服务器的 IP 地址记录在域控制器内的 Active Directory 数据库中。

（4）当 DHCP 服务器启动时，会通过所属域树内的 Active Directory 数据库来检查此台 DHCP 服务器是否已被授权。若已经被授权，该 DHCP 服务器就可以将 IP 地址租给 DHCP 客户端，不论 DHCP 客户端计算机是否隶属于同一域树。

（5）不是域成员的 DHCP 服务器（独立服务器）无法被授权。此台服务器在启动 DHCP 服务时，会检查其所属子网内是否存在任何一台已经在 Active Directory 数据库内被授权的 DHCP 服务器。

- 如果存在的话，这台独立服务器就不会启动 DHCP 服务，也不会出租 IP 地址给 DHCP 客户端。
- 如果不存在的话，这台独立服务器就会正常启动 DHCP 服务，并且可以出租 IP 地址给 DHCP 客户端。如果以后在域上的成员（同一子网）再安装另外一台 DHCP 服务器，则这台独立服务器上的 DHCP 服务将无法再启动。

（6）DHCP 服务器的完全合格域名不可以超过 64 个字符，如果超过 64 个字符、就必须通过 IP 地址来授权。

步骤 5：DHCP服务器配置

在 Windows Server 2003 中，DHCP administrators 和 administrators 组内的成员可以执行 DHCP 服务器的管理工作，如新建作用域、修改作用域、修改配置等。DHCP User 组内的成员可以检查 DHCP 服务器内的数据库与配置，但无权修改。

1）新建作用域

（1）右击 DHCP 服务器的计算机名“xzx-chujl.xpc.edu.cn［192.168.11.240］”，从弹出的菜单中选择“新建作用域”选项，弹出“新建作用域向导”对话框，单击“下一步”按钮，弹出“作用域名”对话框。在这里先建立“子网 1”的作用域。

在“名称”文本框中输入“子网 1”，在“描述”文本框中输入“为子网 1 的用户分配

IP 地址”，如图 8.7 所示。

（2）单击“下一步”按钮，弹出“IP 地址范围”对话框。在“起始 IP 地址”文本框中输入此作用域的开始 IP 地址 192.168.11.2，在“结束 IP 地址”文本框中输入此作用域的结束 IP 地址 192.168.11.254，“长度”文本框中会按照标准掩码自动变为 24，此时“子网掩码”文本框的数值自动为 255.255.255.0，如图 8.8 所示。

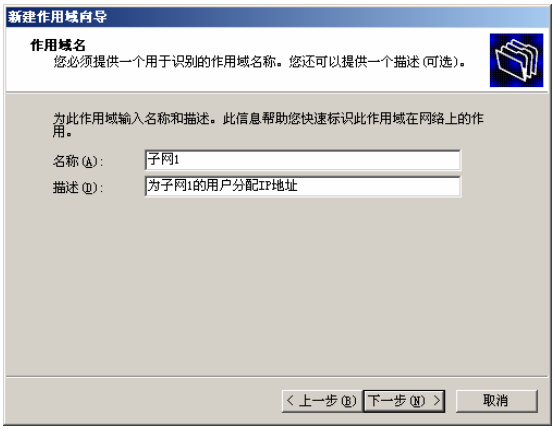

图 8.7 “新建作用域向导”对话框

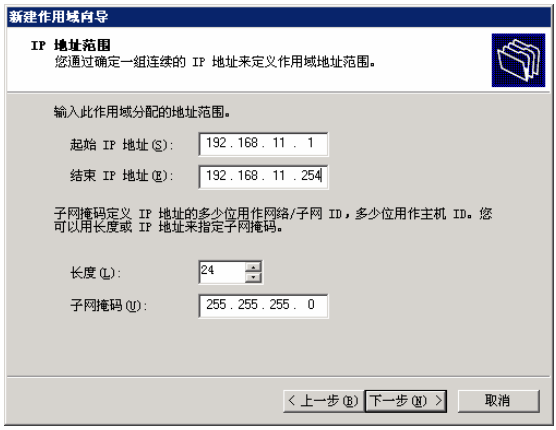

图 8.8 “IP 地址范围”对话框

（3）单击“下一步”按钮，弹出“添加排除”对话框，如图 8.9 所示，可设置在上一步设置的 IP 地址范围中哪一小段 IP 范围不分配给客户机。在此设置排除地址为 192.168.11.60～192.168.11.66，单击“下一步”按钮，弹出“租约期限”对话框，如图 8.10 所示，可设置客户机从 DHCP 服务器租用地址使用的时间，默认为 8 天。

在实际工作中，如果网络中的计算机位置经常变动，如笔记本电脑，则设置较小的租约期限比较好；如果网络中的计算机位置比较固定，如台式计算机，则设置较长的租约期限比较好。

（4）单击“下一步”按钮，弹出“配置 DHCP 选项”对话框，选中“是，我想现在配置这些选项”，单击“下一步”按钮，弹出“路由器（默认网关）”对话框，如图 8.11 所示，在“IP 地址”文本框中输入当前子网的网关地址 192.168.11.1，单击“添加”按钮。

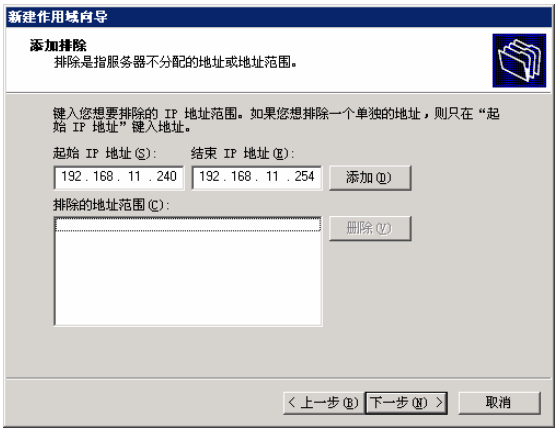

图 8.9 “添加排除”对话框

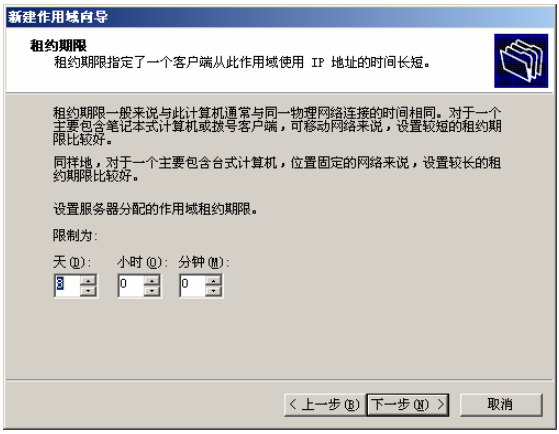

图 8.10 “租约期限”对话框

（5）单击“下一步”按钮，弹出“激活作用域”对话框，选中“是，我想现在激活此作用域”，单击“下一步”按钮，单击“完成”按钮。结束新建作用域的工作，回到 DHCP 控制台，如图 8.12 所示。

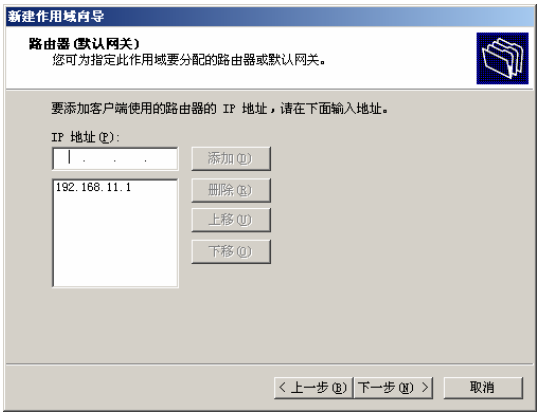

图 8.11　“路由器（默认网关）”对话框

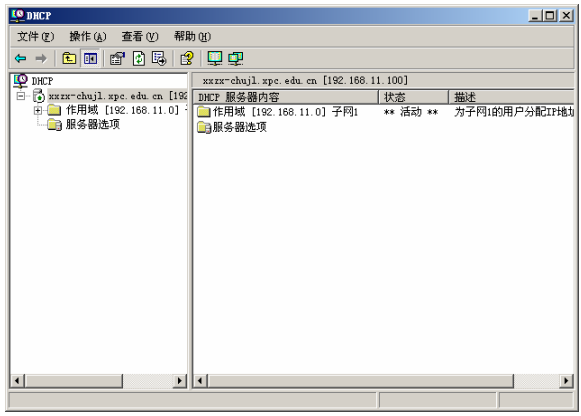

图 8.12　DHCP 控制台

2）修改租约期限

租约期限是指客户端计算机对所获取的 IP 地址配置信息的使用期限。客户端计算机在获取一个 IP 地址后默认只有 8 天的使用期限，使用期限过后需要重新申请一个新的 IP 地址。但在许多情况下并不希望让客户端在这么短的间隔内更换 IP 地址，这时可以通过修改租约期限这个参数，使客户端在获取一个 IP 地址后拥有较长的使用期限或永久使用。租约期限的设置方法如下：

（1）选择“开始→程序→管理工具→DHCP”命令，进入 DHCP 控制台，双击 DHCP 服务器“xxzx-chujl”展开其子项，如图 8.12 所示。

（2）右击“作用域［192.168.11.0］子网 1”，在弹出菜单中选择“属性”选项，弹出“作用域［192.168.11.0］子网 1 属性”对话框，如图 8.13 所示。

在“DHCP 客户端的租约期限”域中的“天”栏中设置天数，如这里设置为 20，即租约期限为 20 天。如选中“无限制”单选项，则拥有永久使用期限。单击“应用”按钮，再单击“确定”按钮，设置完成，然后退出 DHCP 控制台。

3）保留特定 IP 地址给客户端

在 DHCP 服务器中可以为某台计算机指定一个固定地址，将某个 IP 地址和需要固定 IP 的计算机的 MAC 地址进行绑定。也就是说，当这个客户端在向 DHCP 服务器租用 IP 地址或更新租约时，DHCP 服务器都会将相同的 IP 地址出租给此客户端。

（1）获取客户端计算机的 MAC 地址：在命令状态下，执行“ipconfig/all”命令，找到网卡的 MAC 地址。

（2）设置 MAC 地址与固定 IP 地址的绑定：

进入 DHCP 控制台，选择“作用域”子项中的“保留”项，右击鼠标并在弹出的菜单中选择“新建保留”选项，弹出“新建保留”对话框，如图 8.14 所示。在“保留名称”栏中输入一个有一定含义的名字，以便在保留 IP 地址较多时便于管理。在“IP 地址”栏中输入 IP 地址，在“MAC 地址”栏中输入 MAC 地址。单击“完成”按钮，即加入了绑定 MAC 地址和保留的 IP 地址。

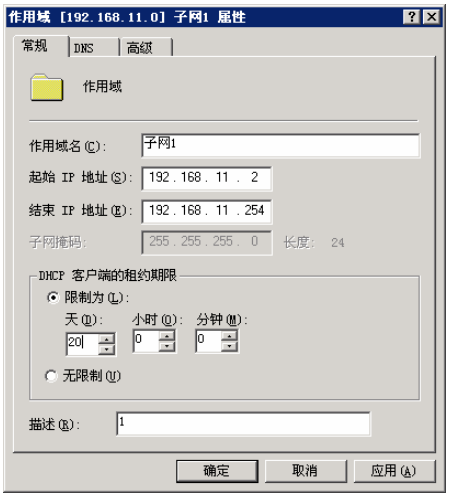

图 8.13 “作用域属性”对话框

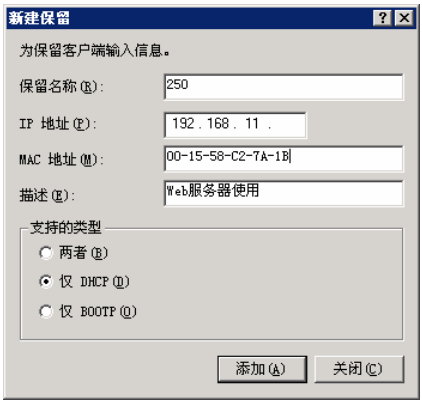

图 8.14 IP 地址和 MAC 地址绑定

4）配置选项

DHCP 服务器除了指定 IP 地址和子网掩码给 DHCP 客户端外，还可以分配一些配置选项给 DHCP 客户端，如 DNS 服务器、默认网关、WINS 服务器等。当 DHCP 客户端在向 DHCP 服务器租用 IP 地址或更新 IP 地址的租约时，DHCP 服务器就可以自动为 DHCP 客户端配置这些选项。

在 DHCP 服务器中有不同等级的 DHCP 选项。

- 服务器选项：服务器选项的配置会自动被所有的作用域来继承。
- 作用域选项：只适合于该作用域。
- 保留：只有当 DHCP 客户端租用到这个保留的 IP 地址时，DHCP 服务器才会替 DHCP 客户端配置这些选项。
- 类别选项：针对某些特定类别的计算机来配置选项。

配置 DNS 服务器选项，在图 8.12 中，展开作用域，右击“作用域”选项，选择“配置”选项，弹出“作用域选项”对话框，勾选“006 DNS 服务器”选项，如图 8.15 所示。

在“IP 地址”处直接输入 DNS 服务器的 IP 地址，单击“添加”、“确定”按钮完成。

如果不知道 DNS 服务器的 IP 地址，可以先在“服务器名”处输入 DNS 服务器的计算机名称，然后单击“解析”按钮让系统查找 DNS 服务器的 IP 地址。

步骤 6：DHCP服务关闭和打开

当需要关闭和打开 DHCP 服务时，有两种方法可以实现：

（1）直接在“DHCP”配置窗口，选择服务器的名字，然后在菜单“操作→所有任务”中，根据需要单击“停止”、“启动”、“暂停”或“重新启动”等。

（2）从“管理工具”中选择“服务”，打开“服务”窗口，可以看到本机所有服务的列表，选择“DHCP Server”，右击，在快捷菜单中根据需要选择“停止”、“启动”、“暂停”或“重新启动”等。

步骤 7：DHCP客户机的配置与测试

（1）DHCP 客户机的配置。DHCP 服务器设置好后，客户机要使用 DHCP 服务器自动提供的 IP 设置，需要进行如下设置：

在“控制面板”中双击“网络和拨号连接”，在弹出的“本地连接”对话框中，单击“属性”按钮，然后单击“Internet 协议（TCP/IP）”选项，单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮，如图 8.16 所示。这样，客户机便成为 DHCP 的客户机，可以使用 DHCP 服务器自动提供的 IP 设置。

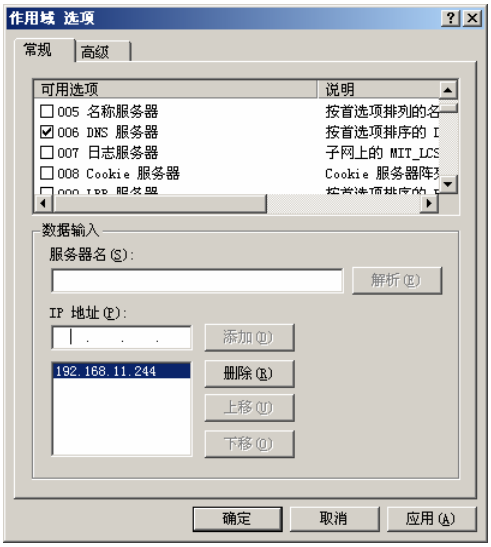

图 8.15　“作用域选项”对话框

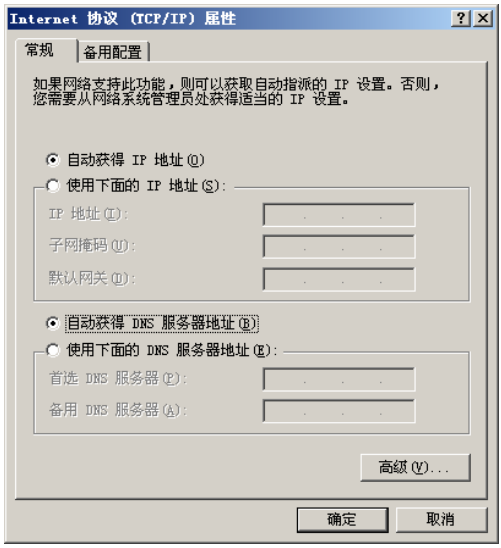

图 8.16　DHCP 客户机的设置

（2）DHCP 客户机的测试。在命令行提示符方式下，利用“ipconfig”命令可查看 IP 地址的获得；利用“ipconfig/all”命令可查看详细的 IP 设置（包括网卡的物理地址）；利用“ipconfig/releasee”命令可释放获得的 IP 地址；利用“ipconfig/renew”命令重新获得 IP 地址。

8.2　任务 2：在一台DHCP服务器上建立多个作用域

因为 DHCP 客户端是通过广播方式来发现 DHCP 服务器，并从 DHCP 服务器中获得 IP 地址的，所以一般一台 DHCP 服务器只为一个 IP 网段提供租用 IP 地址的服务。那么，一台 DHCP 服务器能否为两个或两个以上的 IP 网段提供租用 IP 地址的服务呢？本实训任务将解决这一问题。

8.2.1　任务内容

1．任务目的

通过本实训任务的实施，深入了解 DHCP 的工作原理，以 Windows Server 2003 操作系统为例，掌握同一台 DHCP 服务器为不同子网动态分配 IP 地址的实现方法。

2．实训任务

随着单位局域网内计算机数量的增加，计算机被分配在两个子网内，需要在局域网内部安装并配置一台 DHCP 服务器，为公司内两个子网内除服务器以外的所有计算机自动配置 IP 地址、子网掩码、默认网关、DNS 服务器地址等网络参数。

3．任务目标

（1）了解代理服务器的功能和应用；

（2）理解 DHCP 的基本概念和运行原理；

（3）了解将 Windows Server 2003 计算机作为路由器的特点和配置过程；

（4）学会在 Windows Server 2003 系统下配置 DHCP 中继代理的方法。

8.2.2 相关知识

DHCP 服务器需要为不同网段的 DHCP 客户端分配 IP 地址，而 DHCP 信息是以广播方式进行的，不能穿越到不同的网段，这时可以采用两种方法来解决此问题：

- 在每一个网段都安装一个 DHCP 服务器；
- 利用 DHCP 中继代理来为不在同一网段的 DHCP 客户端分配 IP 地址。

在每一个网段都安装一个 DHCP 服务器在前面已经介绍，在这里介绍通过 DHCP 中继代理来为不在同一网段的 DHCP 客户端分配 IP 地址。

可以在一台 DHCP 服务器内建立多个 IP 作用域，以便对多个子网区段内的 DHCP 客户端提供服务，如果用户 DHCP 服务器与客户机分别位于不同的网段上，则用户的路由器必须具备 DHCP/BOOTP Relay Agent 的功能。Relay Agent 是一个把某种类型的信息从一个网段传播到另一个网段的小程序。DHCP Relay Agent 是一个硬件或程序，它能够把 DHCP/BOOTP 广播信息从一个网段转播到另一个网段上。

下面用一个实例来说明 Relay Agent 的工作过程。

如图 8.17 所示，在子网 2 中的客户机 C 从子网 1 中的 DHCP 服务器上获得 IP 地址租约。

（1）DHCP 客户机 C 在子网 2 上广播 DHCP/BOOTP Discover 消息（DHCP Discover）寻找 DHCP 服务器，广播是将消息以 UDP（User Datagram Protocol）数据报的形式通过 67 端口发出。

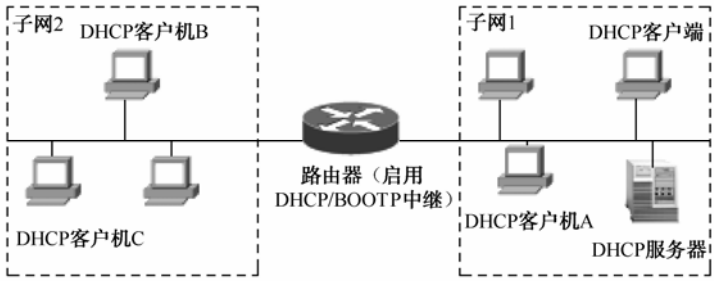

图 8.17　Relay Agent 工作过程

（2）当 Relay Agents（在本例中是一个具有 DHCP/BOOTP Relay Agents 功能的路由器）接收到这个消息后，它检查包含在这个消息报头中的网关 IP 地址，如果 IP 地址为 0.0.0.0，则用 Relay Agent 或路由器的 IP 地址替换它，然后将其转发到 DHCP 服务器所在的子网 1 上。

（3）当在子网 1 中的 DHCP 服务器收到这个消息后，它开始检查消息中的网关 IP 地址是否包含在 DHCP 范围内，从而决定它是否可以提供 IP 地址租约。

如果 DHCP 服务器含有多个 DHCP 范围，消息中的网关 IP 地址是用来确定从哪个 DHCP 范围中挑选 IP 地址并提供给客户的。

（4）DHCP 服务器将它所提供的 IP 地址租约（DHCP Offer）直接发送到 Relay Agent 路由器，并将这个租约利用广播的形式转发给 DHCP 客户机。

8.2.3　方案设计及准备

1．设计

如果路由器没有中继代理的功能，可以在没有 DHCP 服务器的网段内，找一台 Windows Server 2003 计算机，启动 DHCP 中继代理的功能，它就可以将该网段内的 DHCP 信息转发到有 DHCP 服务器的网段内。如图 8.18 所示。

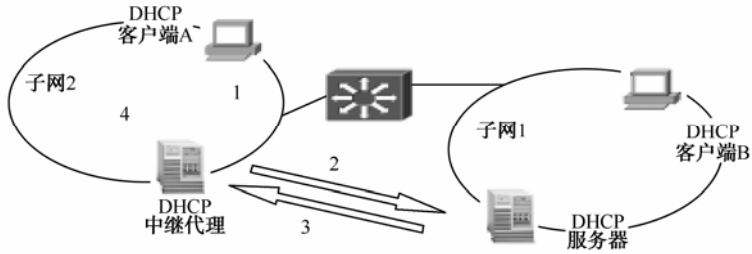

图 8.18　Windows Server 2003 中继代理

在图 8.18 中，子网 2 的 DHCP 客户端 A 通过 DHCP 中继代理从子网 1 的 DHCP 服务器上获得 IP 地址，其运行的过程为：

（1）DHCP 客户端 A 利用广播信息（DHCP Discover）寻找 DHCP 服务器。

（2）DHCP 中继代理收到此信息后，将其直接转发到另一网段的 DHCP 服务器。

（3）DHCP 服务器直接响应信息（DHCP Offer）给 DHCP 中继代理。

（4）DHCP 中继代理将此信息（DHCP Offer）广播给 DHCP 客户端 A。

在图 8.18 中，通过 DHCP 中继代理完成 192.168.11.2～192.168.11.100 和 192.168.12.2～192.168.12.100 两个不同网段之间进行 DHCP 通信的网络拓扑。其中，

（1）这两个网段的子网掩码都为 255.255.255.0。

（2）192.168.11.0/24 网段的网关地址为 192.168.11.1，192.168.12.0/24 网段的网关地址为 192.168.12.1。

（3）DHCP 服务器位于 192.168.11.0/24 子网内，而 192.168.12.0/24 网段的 DHCP 客户端通过运行 Windows Server 2003 的中继代理向位于 192.168.11.0/24 子网内的 DHCP 服务器租用 IP 地址。

（4）DHCP 服务器 IP 地址 192.168.11.240，DHCP 中继代理 IP 地址为 192.168.12.240。

（5）运行 Windows Server 2003 充当路由器的计算机需要两块网卡，分别位于 192.168.11.0/24 和 192.168.12.0/24 两个网段内，网卡地址为网关地址。

根据以上要求，本项目的网络拓扑结构如图 8.19 所示。

图 8.19　DHCP 服务网络拓扑图

2．设备清单

为了搭建如图 8.19 所示的网络环境，需要的设备和连线主要包括：

① 安装 Windows Server 2003 的 PC 计算机 3 台，其中一台需要有两块网卡；

② 测试用计算机 3 台（Windows XP 系统）；

③ 直通线 7 条；

④ 交换机 2 台。

8.2.4 项目实施

步骤 1：硬件连接

按照图 8.19 搭建本实训项目网络环境。

步骤 2：进行TCP/IP设置

因为要配置 DHCP 服务器，客户机通过 DHCP 自动获得 IP 地址等信息，所以客户机不需要配置 IP 地址。而充当 DHCP 服务器、中继代理和路由器的计算机需要设置 IP 地址，其中 DHCP 服务器设置 IP 地址为 192.168.11.240，子网掩码为 255.255.255.0，网关为 192.168.11.1。DHCP 中继代理设置 IP 地址为 192.168.12.240，子网掩码为 255.255.255.0，网关为 192.168.12.1。运行 Windows Server 2003 充当路由器的计算机的两块网卡 IP 地址为：与 192.168.11.0/24 网段相连的网卡的 IP 地址为 192.168.11.1，子网掩码为 255.255.255.0，网关为 192.168.11.1；与 192.168.12.0/24 网段相连的网卡的 IP 地址为 192.168.12.1，子网掩码为 255.255.255.0，网关为 192.168.12.1。

步骤 3：在DHCP服务器添加地址池

在 DHCP 服务器上创建 2 个作用域，创建过程在前面已经介绍过。

步骤 4：启用路由和远程访问

在路由器（安装 Windows Server 2003 的计算机）上配置并启用“路由和远程访问”。

（1）选择“开始→程序→管理工具→路由和远程访问”命令，弹出“路由和远程访问”窗口，鼠标右击服务器名图标，从菜单中选择“配置并启用路由和远程访问”选项，弹出“路由和远程访问服务器安装向导”窗口。

（2）单击“下一步”按钮，弹出“配置”对话框，如图 8.20 所示，选择“自定义配置”选项。

（3）单击“下一步”按钮，弹出“自定义配置”对话框，如图 8.21 所示，选择“LAN 路由”选项。

（4）单击“下一步”按钮，选择开始路由和远程访问服务。当前面的配置无误时，单击“完成”按钮，弹出“路由和远程访问”窗口。

（5）单击“是”按钮，开始启用路由和远程访问服务功能。配置完成后，“路由和远程访问”窗口如图 8.22 所示。

步骤 5：配置DHCP中继代理

在子网 2 中充当中继代理的计算机（安装 Windows Server 2003 操作系统，IP 地址为 192.168.12.200）上配置 DHCP 中继代理。

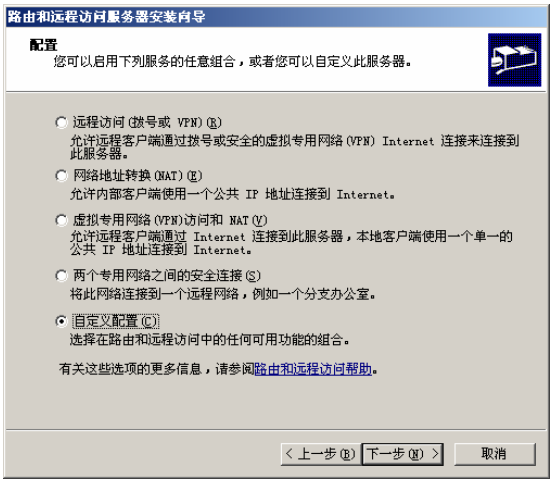

图 8.20　“配置”对话框

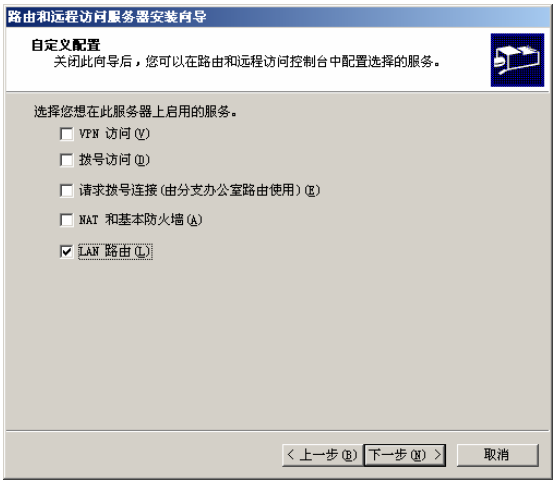

图 8.21　“自定义配置”对话框

（1）选择“开始→程序→管理工具→路由和远程访问”命令，弹出“路由和远程访问”窗口。

（2）选择“IP 路由选择”选项，右击“常规”选项，选择“新增路由协议”选项，弹出“新路由协议”对话框，如图 8.23 所示。

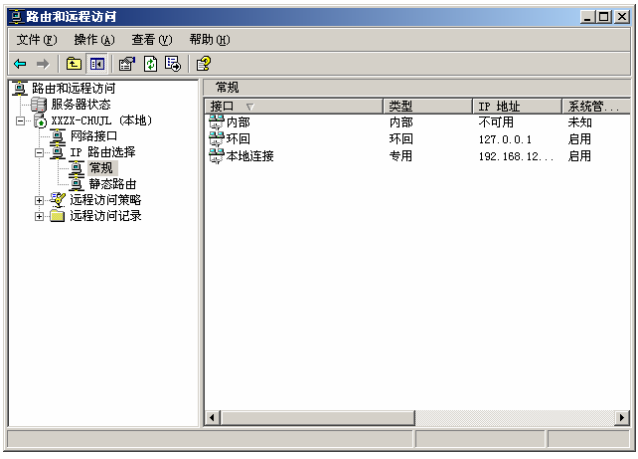

图 8.22　“路由和远程访问”窗口

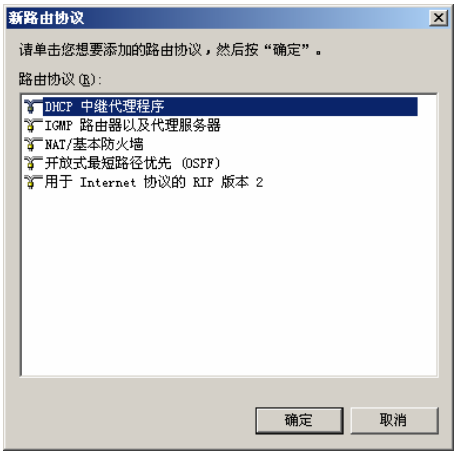

图 8.23　“新路由协议”对话框

（3）选择“DHCP 中继代理程序”选项，单击“确定”按钮。在“IP 路由选择”选项下新增“DHCP 中继代理程序”。

（4）在图 8.22 中，鼠标右击“DHCP 中继代理程序”选项，从弹出的菜单中选择“属性”选项，弹出“DHCP 中继代理程序 属性”对话框，输入 DHCP 服务器的 IP 地址（本例中为 192.168.11.200），单击“添加”按钮，如图 8.24 所示，单击“确定”按钮返回。

（5）在图 8.22 中，鼠标右击“DHCP 中继代理程序”选项，从弹出的菜单中选择“新增接口”选项，弹出“DHCP 中继代理程序 的新接口”对话框。选择“本地连接”（选择提供 DHCP 中继代理的网络接口，当此 DHCP 中继代理程序收到通过此接口传送来的 DHCP 包时，就会将包转发给 DHCP 服务器），单击“确定”按钮，如图 8.25 所示。

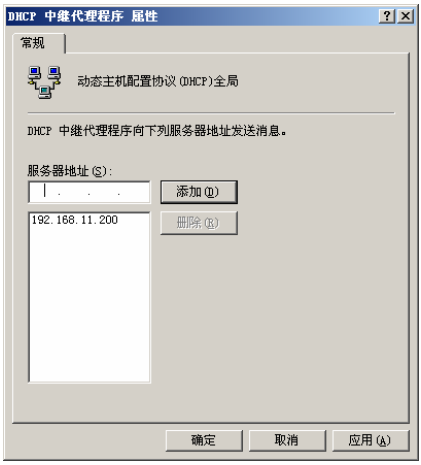

图 8.24　DHCP 中继代理程序属性

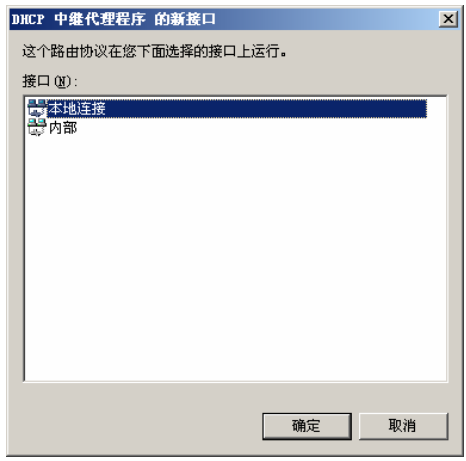

图 8.25　DHCP 中继代理程序的新接口

（6）弹出“DHCP 中继站属性—本地连接 属性”对话框，如图 8.26 所示。单击“确定”按钮，完成配置。

- 跃点计数阈值（hop count threshold）：表示 DHCP 广播信息最多只能够经过多少个路由器来转发。
- 启动阈值（boot threshold）（秒）：在 DHCP 中继代理程序收到 DHCP 信息后，必须等此处所配置的时间过后，才会将信息转发给远程的 DHCP 服务器。

（7）单击“确定”按钮，完成设置。

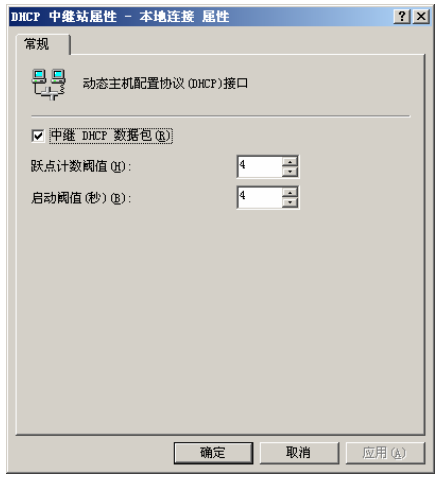

图 8.26　“本地连接属性”对话框

步骤 6：测试验证

此时，在子网 2（192.168.12.0/24）的任何一台 DHCP 客户端的命令提示符下运行“ipconfig/all”命令，可以看到计算机的 IP 地址、默认网关、DHCP 服务器 IP 地址为 192.168.11.200 等。说明 DHCP 客户端已经成功地向另一子网中的 DHCP 服务器租用到了 IP 地址。

8.3　任务 3：DHCP超级作用域的配置与作用

对于一个 C 类网络来说，在同一子网内最大只能容纳 254 台主机，当实际接入的主机数量超过 254 台时，就需要再划分不同的子网。但是，不同子网之间的通信需要路由器或三层交换机，那么能否让一台 DHCP 服务器在同一物理网段中提供多个 IP 子网呢？Windows Server 2003 中的 DHCP 超级作用域提供了此服务。

8.3.1 任务内容

1．任务目的

通过本实训任务的实施，了解 DHCP 超级作用域的应用特点，并掌握在 Windows Server 2003 操作系统中超级作用域的配置方法。

2．实训任务

某公司组建内部局域网，使用一个 C 类地址为网络内的计算机分配地址。随着公司信息化的建设，计算机数量超过了 254 台，但公司只想在局域网内部安装并配置一台 DHCP 服务器，为公司内除服务器以外的所有计算机自动配置 IP 地址、子网掩码、默认网关、DNS 服务器 IP 地址等网络参数。

3．任务目标

① 了解超级作用域的功能特点；
② 学会 DHCP 超级作用域的配置方法；
③ 进一步了解 DHCP 在网络中的作用。

8.3.2 相关知识

超级作用域（Superscope）是由多个作用域组合而成的，它可以被用来支持 multinets 的网络环境。multinets 是在一个实体网络内有多个逻辑的 IP 网络，也就是在实体网络内让不同的计算机有不同的 Network ID，从实体上看这些计算机在同一网段内，但逻辑上却是分别隶属于不同的网络，它们分别有不同的 Network ID。

Windows Server 2003 的 DHCP 服务器可以通过“超级作用域”来将 IP 地址出租给 multinets 内的 DHCP 客户端。

如图 8.27 所示，DHCP 服务器内只有一个作用域，可出租的 IP 地址范围为 192.168.20.2～192.168.20.254，其中的 192.168.20.231～192.168.20.254 被排除。

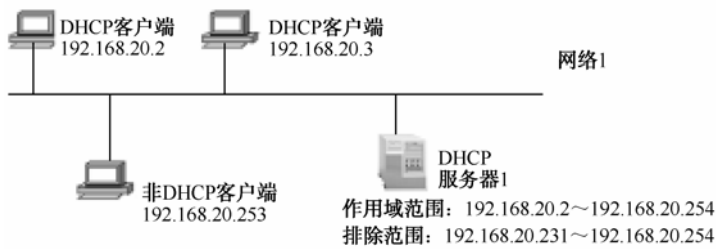

图 8.27　一个作用域的 DHCP 服务器

当图 8.27 中网络 1 的计算机数量越来越多，以至于需要用到第 2 个 Network ID 的 IP 地址时，可以在 DHCP 服务器内建立第 2 个作用域，然后将第 1 个作用域与第 2 个作用域组成一个超级作用域，如图 8.28 所示。当图 8.28 中的 DHCP 客户端向 DHCP 服务器租用 IP 地址时，DHCP 服务器会从超级作用域中的任何一个一般作用域中选择一个 IP 地址。

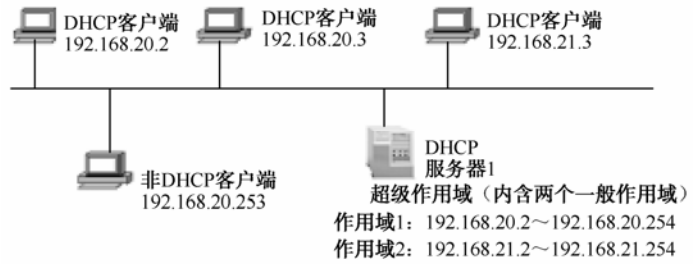

图 8.28　一个作用域的 DHCP 服务器

8.3.3　方案设计及准备

1．设计

假设某公司采用了 192.168.11.0/24 和 192.168.12.0/24 两个网段，架设一台 DHCP 服务器，设计如下：

（1）这两个网段的子网掩码都为 255.255.255.0。

（2）192.168.11.0/24 网段的网关地址为 192.168.11.1，192.168.12.0/24 网段的网关地址为 192.168.12.1。

（3）DHCP 服务器 IP 地址为 192.168.11.240。

根据以上要求，本项目的网络拓扑结构如图 8.29 所示。

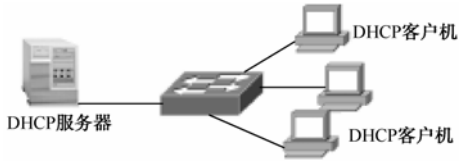

图 8.29　超级作用域拓扑结构图

2．设备清单

为了搭建如图 8.29 所示的网络环境，需要的设备和连线主要包括：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 测试用计算机 3 台（Windows XP 系统）；

③ 直通线 4 条；

④ 交换机 1 台。

8.3.4　项目实施

步骤 1：硬件连接

按照图 8.29 所示搭建本实训项目网络环境。

步骤 2：进行TCP/IP设置

因为要配置 DHCP 服务器，客户机通过 DHCP 自动获得 IP 地址等信息，所以客户机不需要配置 IP 地址。而充当 DHCP 服务器的计算机需要设置 IP 地址，IP 地址为 192.168.11.240，子网掩码为 255.255.255.0，网关为 192.168.11.1。

步骤 3：创建作用域

在 DHCP 服务器上分别创建 192.168.11.2～192.168.11.254 和 192.168.12.2～192.168.12.254 两个作用域。

步骤 4：创建超级作用域

（1）右击 DHCP 服务器，选择“新建超级作用域”选项，弹出“新建超级作用域向导”

对话框，单击“下一步”按钮，弹出“超级作用域名”对话框，输入超级作用域名称，如输入“超级作用域网络 1”，如图 8.30 所示。

（2）单击“下一步”按钮，弹出“选择作用域”对话框，选择其成员（一般作用域），如图 8.31 所示。

图 8.30 “超级作用域名”对话框

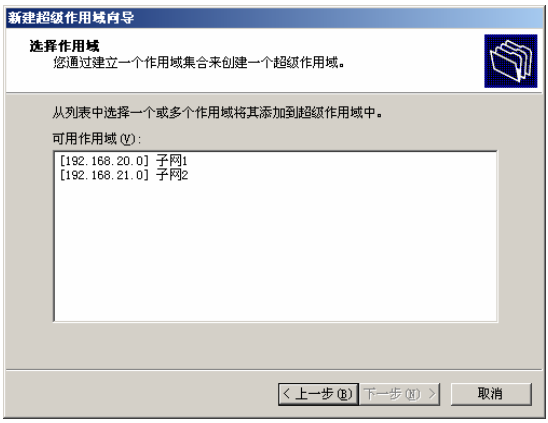

图 8.31 “选择作用域”对话框

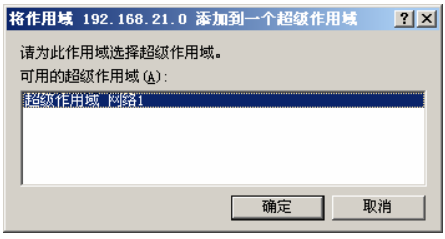

图 8.32 添加作用域到超级作用域

（3）单击“下一步”按钮，完成创建。

（4）在超级作用域中也可以创建新一般作用域，也可以将一般作用域添加到超级作用域。鼠标右击要添加到超级作用域的一般作用域，选择“添加到超级作用域”选项，弹出“将作用域 192.168.21.0 添加到一个超级作用域”对话框，选择要添加到的超级作用域，如图 8.32 所示，单击“确定”按钮完成。

（5）在超级作用域中也可以将一般作用域删除。

步骤 5：验证

同时打开多台（至少 3 台）DHCP 客户端，在命令提示符下运行“ipconfig/all”命令，观察各个计算机的 IP 地址、默认网关等信息。

如果发现这 3 台计算机的地址一直都在 192.168.11.0/24 子网内，原因是在本项目实训中只有两台客户机，而一个子网的 IP 地址就够用了。

8.4 扩展知识及任务训练

8.4.1 安装多台DHCP服务器

可以同时安装多台 DHCP 服务器，以便提供容错的功能，也就是如果其中一台 DHCP 服务器有故障的话，还有其他的 DHCP 服务器可以提供服务。如果网络中有多台 DHCP 服务器，将无法预知是哪一台服务器响应客户机的请求。假设网络上有两台服务器：服务器 1 和服务器 2，分别提供不同的地址范围。如果服务器 1 为客户机提供地址租约，在租期达到 50%时

客户机要与服务器 1 取得通信以便更新租约，如果无法与服务器 1 进行通信，在租期达到87.5%的时候，客户机进入重新申请状态，客户机在子网上发送广播，如果服务器 2 首先响应，由于服务器 2 提供的是不同的 IP 地址范围，它不知道客户机现在使用的是有效的 IP 地址，因此它将发送 DHCP NAK 给客户机，客户机便无法获得有效的地址租约。

一般在建立作用域时建议采用“80/20”的原则。假设在 DHCP 服务器 1 内建立了一个范围为 192.168.16.2～192.168.16.250 的作用域，但是将其中的 192.168.16.200～192.168.16.250 排除，也就是服务器 1 可租给客户端的 IP 地址占用此作用域的 80%；而在 DHCP 服务器 2 内也建立了一个范围为 192.168.16.2～192.168.16.250 的作用域，但是将其中的 192.168.16.2～192.168.16.199 排除，也就是服务器 2 可租给客户端的 IP 地址占用此作用域的 20%。

安装与配置 DHCP 服务器的过程同前面介绍的一样。

8.4.2 DHCP数据库的维护

DHCP 服务器的数据库文件默认是位于%systemroot%\system32\dhcp 文件夹内，如图 8.33 所示，其中的 dhcp.mdb 是其存储信息的文件，其他则是辅助性的文件。

在 DHCP 服务器控制台，右击 DHCP 服务器，选择“属性→高级→数据库路径”选项，可以修改存储数据库的文件夹，如图 8.34 所示。

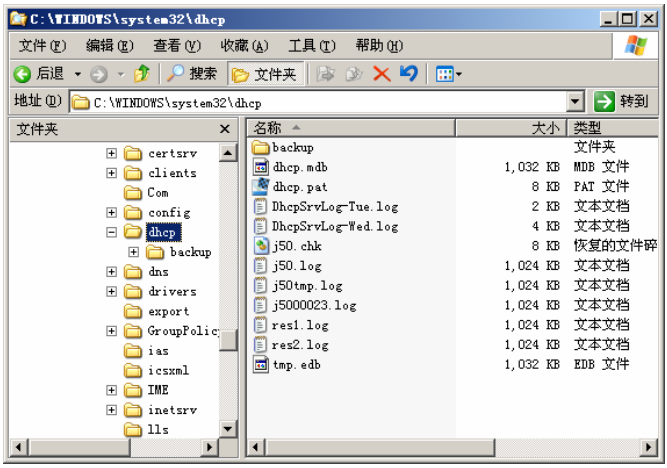

图 8.33 DHCP 数据库文件

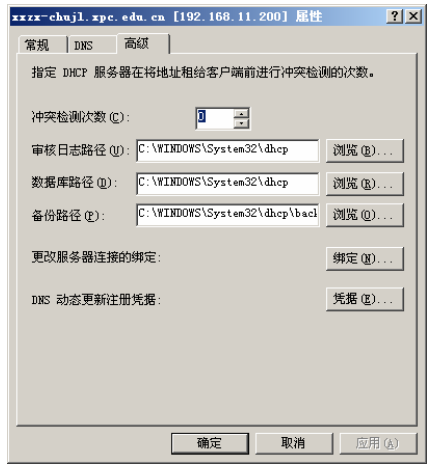

图 8.34 修改存储数据库文件路径

1. 数据库的备份

如果 DHCP 服务器配置信息丢失，可以通过备份文件进行还原。数据库的备份可通过以下两种方式进行。

（1）自动备份：DHCP 服务器默认会每隔 60 分钟自动将 DHCP 数据库文件备份到%systemroot%\system32\dhcp\backup 文件夹内。

可以通过修改注册表的 backupinterval 键值，来更改自动备份时间间隔。

（2）手工备份：鼠标右击 DHCP 服务器，选择“备份”选项，将 DHCP 数据库文件备份到指定的文件夹内。

如果更改 DHCP 数据库文件的备份的默认路径，则自动备份失效。

2．数据库的还原

数据库的还原也可采用两种方式。

（1）自动还原：DHCP 服务如果检测到 DHCP 数据库已损坏，它会自动修复数据库。它利用%systemroot%\system32\dhcp\backup 文件夹内的备份文件来还原。

（2）手工还原：鼠标右击 DHCP 服务器，选择“还原”来还原 DHCP 数据库。

习　题

一、填空题

1．DHCP 的工作过程包括_____、_____、_____、_____4 步。

2．当 IP 地址的租期达到一半的时间时，DHCP 客户端会向 DHCP 服务器发送（非广播方式）一个_____信息，以便续租该 IP 地址。

3．在 DHCP 服务器上建立好作用域后，必须经过_____，该作用域才能开始工作。

4．使用 DHCP 动态分配 IP 地址的网络中，DHCP 客户机的 TCP/IP 参数应该配置为_____IP 地址。

5．使用 DHCP 动态分配 IP 地址时，网络中的某主机要求每次都得到相同的 IP 地址，则应该在 DHCP 服务器的作用域中为该主机建立_____。

二、选择题

1．DHCP 协议的功能是（　　）。

A．为客户自动进行注册　　B．为客户自动配置 IP 地址

C．使 DNS 名字自动登录　　D．为 WINS 提供路由

2．DHCP 客户得到的 IP 地址的时间称为（　　）。

A．生存时间　　B．周期

C．租约期限　　D．存活期

3．DHCP 客户机申请 IP 地址租约时首先发送的信息是（　　）。

A．DHCP Discover　　B．DHCP Offer

C．DHCP Request　　D．DHCP Positive

4．下面哪条命令可以让计算机到 DHCP 服务器上更新 IP 地址？（　　）

A．ipconfig/renew　　B．ipconfig/all

C．pconfig/dhcp　　D．ipconfig/flushdns

5．使用（　　）命令停止 DHCP 服务。

A．net start dhcpserver　　B．jetpack dhcp. mdb

C．net stop dhcpserver　　D．dhcp positive

6．对超级作用域的描述，下面不正确的是（　　）。

A．超级作用域是一个定义了新特性的作用域

B．超级作用域用来实现同一个物理子网中包含多个逻辑 IP 子网

C．超级作用域中只包含一个成员作用域或子作用域的列表

D．超级作用域不用于设置具体的范围，子作用域的各种属性需要单独设置

7．通过运行（　　）命令可以设置在操作系统启动时自动运行 DHCP 服务。

A．ipconfig　　B．touch

C．chkconfig　　D．reboot

8．DHCP 服务采用（　）的工作方式。

A．广播　　B．单播

C．组播　　D．群播

9．动态主机配置协议 DHCP 是对 BOOTP 协议的补充，DHCP 和 BOOTP 的主要区别是 DHCP 具有__①__机制。DHCP 协议支持的中继代理是一种__②__，它可以在两个网段之间传送报文。DHCP 具有多重地址分配方案，对于移动终端最适合的分配方案是__③__。使用 Windows Server 2003 操作系统的 DHCP 客户机，如果启动时无法与 DHCP 服务器通信，它将__④__。因为 DHCP 报文是装入__⑤__协议数据单元中传送的，所以它是不安全的。

① A．动态地址绑定　　B．报文扩充

C．配置参数提交　　D．中继代理

② A．使用 DHCP 协议的路由器　　B．转发 DHCP 报文的主机或路由器

C．可访问到的 DHCP 主机　　D．专用的服务器

③ A．自动分配　　B．动态分配

C．人工分配　　D．静态分配

④ A．借用别人的 IP 地址　　B．任意选取一个 IP 地址

C．在特定网段中选取一个 IP 地址　　D．不使用 IP 地址

⑤ A．TCP　　B．UDP

C．IP　　D．ARP

三、简答题

1．作为 DHCP 服务器的计算机应满足什么条件？

2．如何验证 DHCP 服务器是否工作正常？请设计相应步骤进行验证。

3．简述 DHCP 的工作过程。

4．DHCP 自举向前转发代理用在什么地方？

项目 9　利用IIS架设单位内部Web服务器

Internet 信息服务(Internet Information Server，IIS)是 Windows NT/2000/2003 操作系统中提供的 Web 服务系统，主要用于提供 Web 站点的发布、使用和管理等功能，Windows Server 2003 集成了 IIS 6.0 服务组件。

9.1　项目内容

1．项目目的

在熟悉 Web 工作原理的基础上，学习并掌握基于 Windows Server 2003 的 IIS 服务的安装和基本配置方法。

2．项目任务

有一所高等院校，组建了校园网，开发了学院网站，需要架设一台 Web 服务器来运行学院网站，为学校内部和互联网用户提供浏览服务。

3．任务目标

① 熟悉 Web 应用的工作原理；
② 熟悉 HTTP 和 HTML 协议的工作原理和应用特点；
③ 学会 IIS 6.0 组件的安装与卸载；
④ 学会利用 IIS 6.0 进行网站建立的方法；
⑤ 学会 IIS 6.0 网站的配置和管理过程。

9.2　相关知识

9.2.1　WWW服务概念及服务原理

万维网（World Wide Web，WWW）服务，又称为 Web 服务，是目前因特网上最方便和最受欢迎的信息服务类型，是因特网上发展最快同时又是使用最多的一项服务，目前已经进入广告、新闻、销售、电子商务与信息服务等诸多领域，它的出现是 TCP/IP 互联网发展中的一个里程碑。

WWW 服务采用客户/服务器工作模式，客户机即浏览器（Browser），服务器即 Web 服务器，它以超文本标记语言（HTML）和超文本传输协议（HTTP）为基础，为用户提供界面一致的信息浏览系统。信息资源以页面（也称网页或 Web 页面）的形式存储在 Web 服务器上（通常称为 Web 站点），这些页面采用超文本方式对信息进行组织，页面之间通过超链接连接起来。这些通过超链接连接的页面信息既可以放置在同一主机上，也可以放置在不同的主机上。超链接采用统一资源定位符（URL）的形式。WWW 服务原理是用户在客户机通过

浏览器向 Web 服务器发出请求，Web 服务器根据客户机的请求内容将保存在服务器中的某个页面发回给客户机，浏览器接收到页面后对其进行解释，最终将图、文、声等并茂的画面呈现给用户。WWW 服务原理如图 9.1 所示。

WWW 由遍布在因特网中的被称为 WWW 服务器（又称为 Web 服务器）的计算机组成。Web 是一个容纳各种类型信息的集合，从用户的角度看，万维网由庞大的、世界范围的文档集合而成，简称为页面（page）。

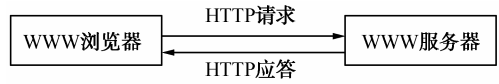

图 9.1　WWW 服务原理

用户使用浏览器总是从访问某个主页（Homepage）开始的。由于页中包含了超链接，因此可以指向另外的页，这样就可以查看大量的信息。

9.2.2　统一资源定位符URL

1．URL的格式

统一资源定位符（Uniform Resource Locator，URL）是对可以从因特网上得到的资源的位置和访问方法的一种简洁的表示。URL 给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。只要能够给资源定位，系统就可以对资源进行各种操作，如存取、更新、替换和查找其属性。

上述的“资源”是指在因特网上可以被访问的任何对象，包括文件目录、文件、文档、图像、声音等，以及与因特网相连的任何形式的数据。

URL 相当于一个文件名在网络范围的扩展。因此，URL 是与因特网相连的机器上的任何可访问对象的一个指针。由于对不同对象的访问方式不同（如通过 WWW、FTP 等），所以 URL 还能指出读取某个对象时所使用的访问方式。URL 的一般形式为：

<URL 的访问方式>：//<主机域名>:<端口>/<路径>

其中：

- <URL 的访问方式>用来指明资源类型，除了 WWW 用的 HTTP 协议之外，还可以是 FTP、News 等。
- <主机域名>表示资源所在机器的主机名字，是必需的。主机域名可以是域名方式，也可以是 IP 地址方式。
- <端口>和<路径>有时可以省略。
- <路径>用来指出资源在所在机器上的位置，包含路径和文件名，通常格式为“目录名/目录名/文件名”，也可以不含有路径。例如，http：//www.xpc.edu.cn/。

在输入 URL 时，资源类型和服务器地址不区分字母的大小写，但目录名和文件名则可能区分字母的大小写。这是因为大多数服务器安装了 UNIX 操作系统，而 UNIX 的文件系统区分文件名的大小写。

2．使用HTTP的URL

对于万维网网站的访问要使用 HTTP 协议。HTTP 的 URL 的一般形式为：

http://<主机域名>：<端口> / <路径>

HTTP 的默认端口号是 80，通常可以省略。若再省略文件的<路径>项，则 URL 就指到因特网上的某个主页（Homepage）。

例如，可以先进入网站主页，URL 为：

```
http://www.xpc.edu.cn
```

更复杂一些的路径是指向层次结构的从属页面。例如：

```
http://www.xpc.edu.cn/xxzx/index.htm
```

用户使用 URL 不仅能够访问万维网的页面，而且能够通过 URL 使用其他的因特网应用程序，如 FTP、Gopher、Telnet、电子邮件及新闻组等。并且，用户在使用这些应用程序时，只使用一个程序，即浏览器。

9.2.3 超文本传输协议HTTP

超文本传输协议 HTTP（Hypertext Transfer Protocol）是用来在浏览器和 WWW 服务器之间传送超文本的协议。HTTP 协议由两部分组成：从浏览器到服务器的请求集和从服务器到浏览器的应答集。HTTP 协议是一种面向对象的协议，为了保证 WWW 客户机与 WWW 服务器之间通信不会产生二义性，HTTP 精确定义了请求报文和响应报文的格式。

- 请求报文：从 WWW 客户向 WWW 服务器发送的请求报文。
- 响应报文：从 WWW 服务器到 WWW 客户的回答。

HTTP 会话过程包括 4 个步骤：连接、请求、应答、关闭。如图 9.2 所示，每个万维网站点都有一个服务器进程，它不断地监听 TCP 的 80 端口，以便发现是否有浏览器（即客户进程）向它发出连接建立请求，一旦监听到连接建立请求并建立了 TCP 连接之后，浏览器就向服务器发出浏览某个页面的请求，服务器接着返回所请求的页面作为响应。最后，TCP 连接就被释放了。在浏览器和服务器之间的请求和响应的交互，必须按照规定的格式和遵循一定的规则。这些格式和规则就是超文本传送协议 HTTP。

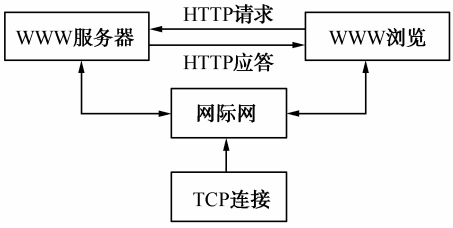

图 9.2 HTTP 会话过程

WWW 以客户/服务器模式进行工作。运行 WWW 服务器程序并提供 WWW 服务的机器被称为 WWW 服务器；在客户端，用户通过浏览器来获得 WWW 信息服务。常用的浏览器有 Mosaic、Netscape 和微软的 IE（Internet Explorer）。

用户浏览页面的方法有两种：一种方法是在浏览器的地址窗口中输入所要找的页面的 URL；另一种方法是在某一个页面中单击一个可选部分，这时浏览器自动在因特网上找到所要链接的页面。

对于每个 WWW 服务器站点都有一个服务器监听 TCP 的 80 端口，看是否有从客户端（通常是浏览器）过来的连接。当客户端的浏览器在其地址栏里输入一个 URL 或者单击 Web 页上的一个超链接时，浏览器就要检查相应的协议，以决定是否需要重新打开一个应用程序，同时对域名进行解析，获得相应的 IP 地址。然后，以该 IP 地址并根据相应的应用层协议，即 HTTP 所对应的 TCP 端口，与服务器建立一个 TCP 连接。连接建立之后，客户端的浏览器使用 HTTP 协议中的“GET”功能向 WWW 服务器发出指定的 WWW 页面请求，服务器收到该请求后将根据客户端所要求的路径和文件名使用 HTTP 协议中的“PUT”功能将相应 HTML 文档送回客户端，如果客户端没有指明相应的文件名，则由服务器返回一个默认的 HTML 页面。页面传送完毕则中止相应的会话连接。

下面以一个具体的例子来介绍 Web 服务的实现过程。假设有用户要访问 http://

www.xpc.edu.cn/index.asp，则浏览器与服务器的信息交互过程如下：

① 浏览器确定Web 页面URL，即 http://www.xpc.edu.cn/index.asp；

② 浏览器请求 DNS 解析 Web 服务器 www.xpc.edu.cn 的 IP 地址，如解析为 192.168.11.250；

③ 浏览器向主机 192.168.11.250 的 80 端口请求建立一条 TCP 连接；

④ 服务器对连接请求进行确认，连接建立的过程完成；

⑤ 浏览器发出请求页面报文，如 GET/index.asp；

⑥ 服务器 192.168.11.250 以 index.asp 页面的具体内容响应浏览器；

⑦ WWW 服务器关闭 TCP 连接；

⑧ 浏览器将页面 index.asp 中的文本信息显示在屏幕上；

⑨ 如果 index.asp 页面上包含图像等非文本信息，那么浏览器需要为每个图像建立一个新的 TCP 连接，从服务器获得图像并显示。

9.2.4 动态网站和Web应用程序

动态网站是指服务器和浏览器之间能够进行数据交互的网站，也称为互动网站。动态网站一般都配置了用于数据处理的 Web 应用程序。

在最初的因特网上，网页是静止的，即 Web 服务器只是简单地把存储的 HTML 文本文件及其引用的图形文件发送给浏览器。只有网页编辑人员使用文字处理器和图形编辑器对它们进行修改后，它们才会发生改变。

后来 Netscape 公司推出了 JavaScript，Sun 公司推出了 Java，网页页面有了一些动态变化，但在服务器端仍旧没有动态变化。直到出现了 CGI、ISAPI 和 ASP 等动态网站技术，Web 服务器才可向浏览器传送动态变化的内容。

根据发生动态改变的位置，将动态技术分为客户端和服务器端两种类型。

客户端的动态技术即浏览器端的动态技术，是指不依赖 Web 服务器，就可直接在浏览器端发生动态改变，并且动态改变的内容与服务器端无关。如常见的脚本动画、翻滚图像效果等。常用的客户端动态技术有 DHTML、Java 小程序和 ActiveX 控件等。

服务器端的动态技术是指在服务器端发生的动态改变，改变后的结果仍然以 HTML 形式发回浏览器。常见的 Web 数据库查询、用户登记等都要用到服务器端的动态技术。常见的服务器端的动态技术有 CGI、ISAPI 和服务器端脚本。

Web 应用程序主要是由服务器端的动态技术实现的。目前最有影响的是微软公司的.net 和 Sun 及 IBM 等公司支持的 J2EE。

9.2.5 Web服务器软件的选择

运行 Web 服务的主流操作系统有两大类：一是 UNIX 家族，如 Linux、Sun Solaris、HP_UX 等，都属于该家族的成员，但相互之间兼容性差；二是 Windows 平台，主要是 Windows Server 2000 和 Windows Server 2003。

NCSA、CERN、Apache 和 Sambar 等都是比较著名的免费 Web 服务器软件。其中 Apache 是目前最为流行的，它能提供快速、可靠的 WWW 服务，源代码完全开放，能够完全胜任每天有数百万人次访问的大型网站，支持 UNIX、Windows 等多种操作系统平台。微软公司有自己 Web 服务器产品——IIS，如果选择微软的 Windows 平台，那么 Web 服务器最好选用 IIS。

9.3 方案设计及准备

1．设计

某单位内部局域网要提供 IIS 服务，以便用户能够方便地浏览单位网站。要求如下：

服务器端：在上一台安装 Windows Server 2003 的计算机（IP 地址为 192.168.11.250，子网掩码为 255.255.255.0，网关为 192.168.11.1）上设置 1 个 Web 站点，要求端口为 80，Web 站点标志为“默认网站”；连接限制为 200 个，连接超时 600s；启用带宽限制，最大网络使用率 1024 KB/s；创建一个名为 xpc 的网站，主目录为 D:\xpcWeb，允许用户读取和下载文件访问，默认文档为 default.asp，网站域名为 http://www.xpc.edu.cn。

客户端：在 IE 浏览器的地址栏中输入 http://192.168.11.250，访问刚才创建的 Web 站点。配合上一章 DNS 服务器的配置，将 IP 地址 192.168.11.250 与域名 www. xpc.edu.cn 对应起来，然后在 IE 浏览器的地址栏中输入 http://www.xpc.edu.cn，访问刚才创建的 Web 站点。

根据以上要求，本项目实施的网络拓扑图如图 9.3 所示。

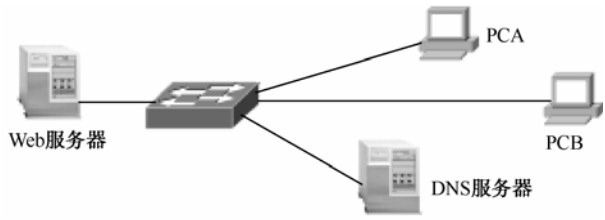

图 9.3　Web 服务网络拓扑图

2．设备清单

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 测试用计算机 1 台（Windows XP 等系统）；

③ 以上两台计算机已连入校园网。

9.4 项目实施

步骤 1：硬件连接

按照图 9.3 搭建 Web 服务器配置网络模型图。

步骤 2：设置IP地址及测试连通性

设置各计算机的 IP 地址、子网掩码、网关如表 9.1 所示。

表 9.1　计算机网络设置信息

计算机	IP 地址	子网掩码	网关
DNS 服务器	192.168.11.244	255.255.255.0	192.168.11.1
Web 服务器	192.168.11.250	255.255.255.0	192.168.11.1
PCA	192.168.11.10	255.255.255.0	192.168.11.1
PCB	192.168.11.11	255.255.255.0	192.168.11.1

使用 ping 测试各计算机之间的连通性。如果全通，继续进行，否则检测网线及计算机的配置，直到各计算机之间全部连通。

步骤 3：IIS 6.0 的安装

Windows Server 2003 默认不会自动安装 IIS，需要自行安装，在安装之前要确认以下事宜：

- IIS 计算机的 IP 地址是静态的，在此处设置 IP 地址为 192.168.11.250，子网掩码为 255.255.255.0，网关为 192.168.11.1；
- 为此网站按照项目 5 中的步骤设置一个 DNS 域名；
- 网页最好存储在 NTFS 磁盘分区中，通过 NTFS 权限来增加网页的安全性。

在 Windows Server 2003 中添加 IIS 的方法如下：

（1）选择“控制面板→添加/删除程序→添加/删除 Windows 组件→组件→Windows 组件向导→应用程序服务器→详细信息”命令，弹出“应用程序服务器”对话框，如图 9.4 所示，选中“ASP.NET”、“Internet 信息服务”复选框，单击“详细信息”按钮，在弹出的“Internet 信息服务”对话框中，选中“公用文件”和“万维网服务”复选框，再次单击“详细信息”按钮，在弹出的“万维网服务”对话框中选中“Active Server Pages”、“万维网服务”、“远程管理（HTML）”复选框，然后单击 3 次“确定”按钮。

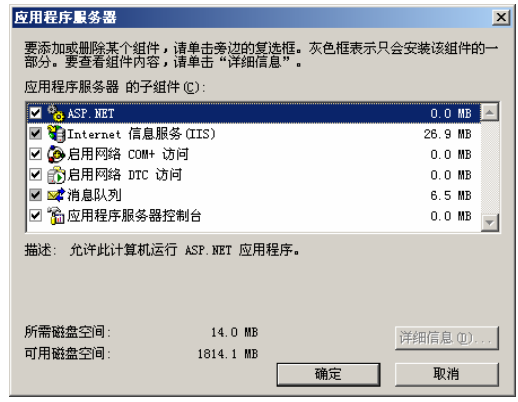

图 9.4　“应用程序服务器”对话框

（2）Windows 组件向导会完成 IIS 的安装，从 Windows Server 2003 安装光盘中复制所需文件。

（3）自行安装 IIS 时，它会被安装成最安全与“锁定”的状态，IIS 默认值提供静态属性服务。如果需要动态属性的话，需要自行解除锁定或安装相关组件。

步骤 4：测试IIS是否安装成功

完成安装后，可以通过“IIS 管理器”来管理网站。

在 Windows Server 2003 中，提供了 Internet 服务管理器来对 IIS 6.0 进行管理，以系统管理员身份登录服务器，选择“开始→程序→管理工具→Internet 信息服务（IIS）管理器”命令，打开“Internet 信息服务管理器”窗口，如图 9.5 所示。从图中可以看出已经有一个网站：

“默认网站”。

在另一台计算机上，利用 IE 来连接与测试网站。测试方法有以下几种：

- 利用 DNS 网址 http://www.xpc.edu.cn 来连接网站；
- 利用 IP 地址 http://192.168.11.250 来连接网站；
- 利用计算机名称 http://server1 来连接网站，这种方法适合于局域网内的计算机。

若连接成功，则应该弹出如图 9.6 所示的网页。

如果没有出现图 9.6 所示的页面，请检查图 9.5 中的“默认网站”右方是否显示有“服务正在运行”。若处于停止状态，右击“默认网站”，选择“启动”来激活此网站。

图 9.5　Internet 信息服务（IIS）管理器窗口

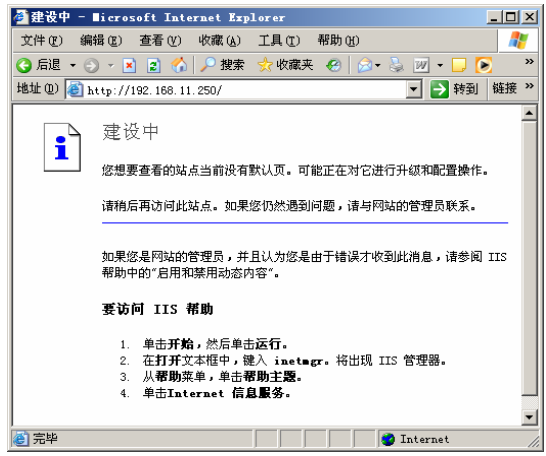

图 9.6　IIS 测试成功

步骤 5：全局性IIS服务器管理

1）全局性的 IIS 服务器属性设置

IIS 服务器属性设置是宏观层次的，具有全局性，其属性设置将作用于其所有的 IIS 服务。展开 IIS 管理器，用鼠标右键单击相应的服务器，选择“属性”选项，打开属性设置对话框，如图 9.7 所示。

默认情况下，IIS 6.0 以本地字符集格式记录日志。如选中“用 UTF-8 编码 Web 日志”复选框，则 IIS 6.0 服务器上的所有网站都将以 UTF-8 格式记录日志。

2）注册 MIME 类型

下面以注册 ISO 扩展名为例，来介绍注册 MIME 具体类型的方法，操作步骤如下：

① 在“Internet 信息服务管理器”窗口中，右击“xxzx-chujl（本地计算机名）”，从弹出的菜单中选择“属性”选项，打开“IIS 属性”对话框，如图 9.7 所示。

② “允许直接编辑配置数据库”也称为“运行时编辑”，选择该复选框可以在 IIS 运行时更改配置数据库属性值，且更改立即生效。可以通过常用的文本编辑工具实现对配置数据库的更改。

③“UTF-8 日志”用来让 IIS 6.0 支持 UTF-8 格式书写的日志文件，而不仅仅支持 ASCII（或本地代码页）格式。IIS 6.0 不支持 FTP 站点的 UTF-8 日志记录。当启用该功能时，IIS 服务器上的所有网站都将以 UTF-8 格式记录日志。否则，IIS 将以本地字符集格式记录日志。

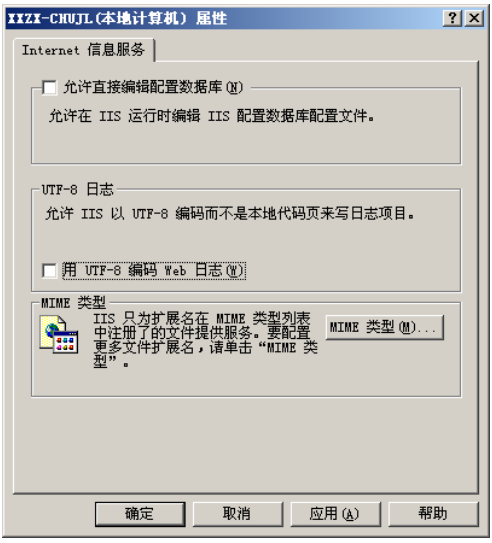

图 9.7 “IIS 属性”对话框

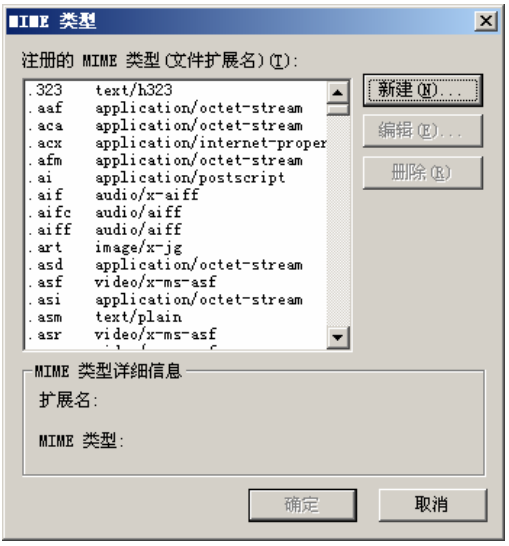

图 9.8 “MIME 类型”对话框

④ 单击“MIME 类型”按钮，弹出“MIME 类型”对话框，如图 9.8 所示。在此对话框中列出了 IIS 6.0 默认支持的 MIME 类型。单击“新建”按钮，打开“新建 MIME 类型”对话框，如图 9.9 所示。在“扩展名”文本框中输入“.ISO”，在“MIME 类型”文本框中输入“application/octet-stream”，然后单击“确定”按钮完成添加。

图 9.9 “新建 MIME 类型”对话框

如果希望处理所有文件而不考虑文件扩展名，则需要添加通配符“*”。完成后从服务中重新启动“IIS Admin Service”服务。

3）全局 WWW 服务属性设置

全局 WWW 服务设置是比 IIS 服务器低一级的层次，它对所有 Web 网站具有全局性。展开 IIS 管理器，右击“网站”，选择“属性”选项，打开“网站属性”对话框，如图 9.10 所示。

这里的属性设置将作用于其所有的 Web 网站。一般情况下采用默认设置，然后再根据需要对某一特定网站进行属性设置。

4）IIS 启动

当 IIS 出现故障后，可以不重新启动计算机而只启动 IIS。右击“Internet 信息服务”树下的主机，在弹出的菜单中执行“所有任务→重新启动 IIS”选项即可。如图 9.11 所示。

5）IIS 6.0 的备份与还原

IIS 6.0 在运行的过程中会自动备份，并且每更改一次 IIS 的设置，IIS 都会自动备份。当 IIS 出现问题时，也可以从以前的备份中恢复设置。

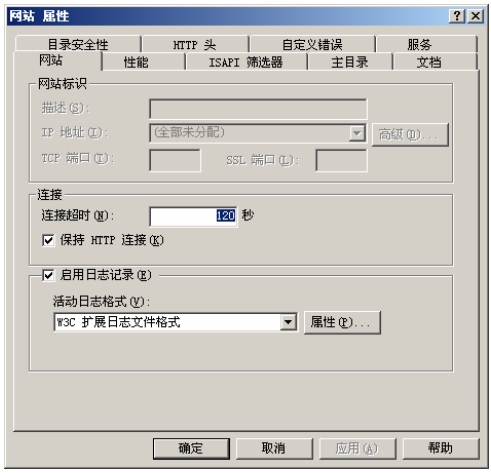

图 9.10 “网站属性”对话框

图 9.11 重新启动 IIS

①右击 IIS 计算机名，从弹出的菜单中选择“所有任务→备份/还原配置”命令。弹出“配置备份/还原”对话框，如图 9.12 所示。默认情况下，IIS 已经为每次的更改创建了备份。此时“还原”和“删除”按钮不可用。

② 单击“创建备份”按钮，弹出“配置备份”对话框，如图 9.13 所示，在“配置备份名称”文本框中输入备份名称，如 dzx，如果需要，可以选择“使用密码加密备份”复选框并输入密码。单击“确定”按钮，刚才配置的备份文件名称“dzx”会自动加入“配置备份/还原”对话框中，此时“还原”和“删除”按钮变为可用。

③ 如果想恢复备份，在“配置备份/还原”对话框中选择想要恢复的配置，单击“还原”按钮，开始恢复。

图 9.12 “配置备份/还原”对话框

图 9.13 “配置备份”对话框

步骤 6：建立单位网站

1）绑定网站 IP 地址

（1）打开“本地连接属性”对话框，选择“Internet 协议（TCP/IP）”选项，单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框。

（2）单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，单击“IP 地址”标签下的“添加”按钮，打开“TCP/IP 地址”对话框，输入 IP 地址和子网掩码，如 IP 地址为 192.168.11.250，子网掩码为 255.255.255.0。如图 9.14 所示。

（3）单击“添加”按钮，返回“高级 TCP/IP 设置”对话框，单击“确定”按钮，再单击“确定”按钮完成设置。

2）建立文件夹

在 D 盘的根目录上创建一个文件夹 xpcweb，然后把网站文件复制到此文件夹内。

3）建立网站 xpc

（1）选择“开始→管理工具→Internet 信息服务(IIS)管理器”选项，打开“Internet 信息服务（IIS）管理器”窗口。

（2）右击“默认网站”选项，在快捷菜单中选择“新建→网站”命令，打开“网站创建向导”对话框，单击“下一步”按钮，打开“网站描述”对话框，如图 9.15 所示。

图 9.14　添加 IP 地址

（3）输入网站的名称，单击“下一步”按钮，打开“IP 地址和端口设置”对话框，如图 9.16 所示。

图 9.15　“网站描述”对话框

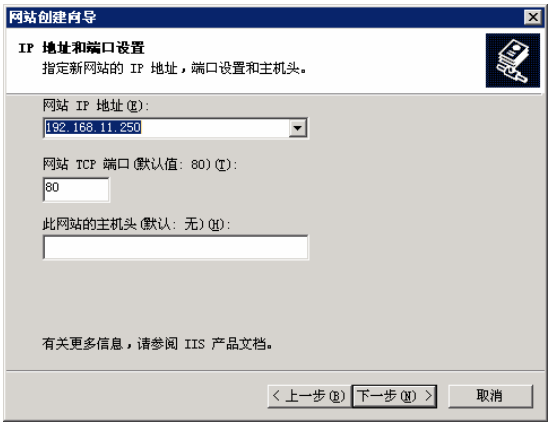

图 9.16　“IP 地址和端口设置”对话框

（4）在“网站 IP 地址”框中选择地址“192.168.11.250”，单击“下一步”按钮，打开“网站主目录”对话框，如图 9.17 所示。

（5）在“路径”文本框中输入网站文件所在的文件夹“D:\xpcweb”，选中“允许匿名访问网站”复选框，单击“下一步”按钮，打开“网站访问权限”对话框，如图 9.18 所示。

（6）设定网站的访问权限，单击“下一步”按钮，完成网站的建立。

图 9.17 “网站主目录”对话框

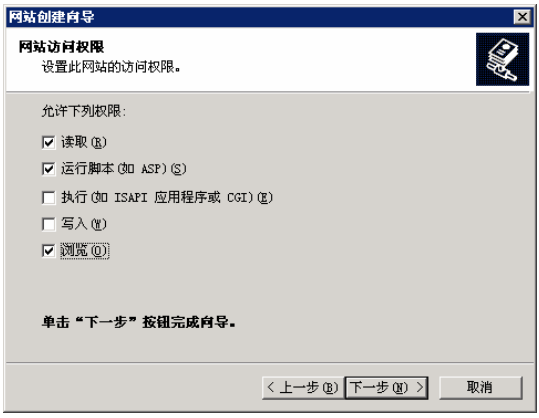

图 9.18 “网站访问权限”对话框

4）设置网站属性

（1）在“Internet 信息服务（IIS）管理器”窗口，单击“网站”，然后用鼠标右键单击前面建立的网站 xpc，在快捷菜单中选择“属性”命令，打开 xpc 属性对话框，如图 9.19 所示。

（2）单击“文档”选项卡，选中“启用默认内容文档”，单击“添加”按钮，打开“添加内容页”对话框，如图 9.20 所示。在“默认内容页”文本框中输入“default.asp”。

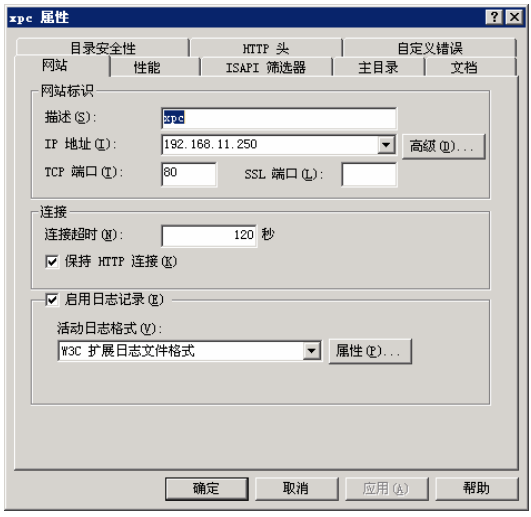

图 9.19 “xpc 属性”对话框

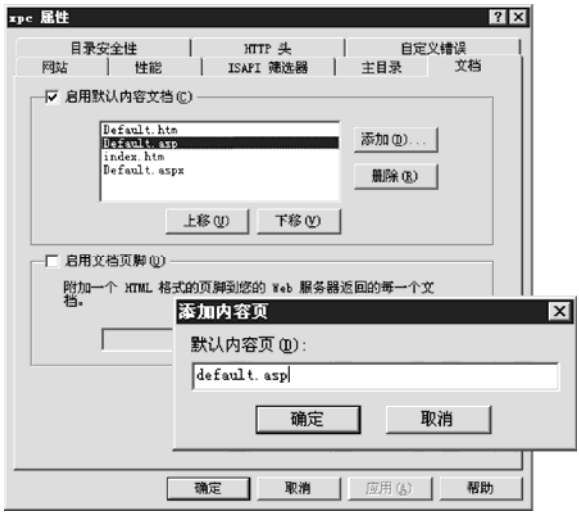

图 9.20 添加默认文档

所谓默认文档，是指在 Web 浏览器中输入 Web 网站的 IP 地址或域名，而不用输入具体的网页文件名时即可显示出来的 Web 页面，也就是通常所说的主页（Homepage）。IIS 6.0 默认的主页文档文件名为 default.htm、default.asp、index.htm 和 default.aspx。如果 Web 网站无法找到这两个文件中的任何一个，那么，将在 Web 浏览器上显示“该页无法显示”的提示。默认文档既可以是一个，也可以是多个。当设置多个默认文档时，IIS 将按照排列的先后顺序依次调用这些文档。当第一个文档存在时，将直接把它显示在用户的浏览器上，而不再调用后面的文档；当第一个文档不存在时，则将第二个文件显示给用户，依次类推。

如果要改变默认文档的搜索顺序，在默认文档列表中选中欲调整位置的文件名，单击“↓”“↑”箭头即可调整其先后顺序。若欲将该文件名作为网站首选的默认文档，须将其调

整至最顶端。

如果要删除默认文档，在默认文档列表中选中欲删除的文件名，并单击“删除”按钮，即可将其删除。

文档页脚（footer）是一种特殊的 HTML 文件，用于使网站中全部的网页上都出现相同的标记。一些大公司通常使用文档页脚将公司徽标添加到其网站中全部网页的上部或下部，以增加网站的整体感。为了使用文档页脚，首先要选择“文档”选项卡中的“启用文档页脚”复选框，然后单击“浏览”指定页脚文件，文档页脚文件通常是一个.htm 格式的文件。

5）在 DNS 服务器建立相应记录

打开 DNS 窗口，右键单击“正向查找区域”，选择快捷菜单中的“新建区域”选项，建立区域 xpc.edu.cn，在新建区域内添加一条主机记录，主机名为 host，IP 地址为 192.168.11.250。

步骤 7：新建虚拟目录

对一个小型网站来说，可以将所有网页与相关文件都存放到网站的主目录之下，也就是在主目录之下建立子文件夹，然后将文件放到这些子文件夹内。这些子文件夹称为“物理目录”。

也可以将文件存储到其他文件夹内，这个文件夹可以位于本地计算机内的其他磁盘驱动器内或是其他计算机内，然后通过“虚拟目录（Virtual Directory）”映射到这个文件夹，每一个虚拟目录都有一个别名（alias）。虚拟目录的好处是在不需要改变别名的情况下，可以随时改变其所对应的文件夹。

利用虚拟目录可为多个用户提供主页发布，这些用户建立各自的虚拟目录，共享同一网站。用户只需在网站域名后加上虚拟目录名，即可区分不同用户的发布内容，这时用户就不能拥有自己独立的域名。

物理目录就是直接在文件系统中创建的真实目录，它可映射为不同的主目录或虚拟目录。用户可以直接在 Windows 系统中创建和删除物理目录，也可在 IIS 管理器中管理物理目录。在 IIS 管理器中展开某个主目录或虚拟目录时，其对应的物理目录中的内容也将显示出来。用户可选择某个主目录或虚拟目录，右击“资源管理器”，打开资源管理器创建目录。

虚拟目录和物理目录（不带别名的目录）都显示在 IIS 管理器中。虚拟目录用齿轮图标来表示，对于浏览器，虚拟目录显示为主目录（根）的子目录，必须为浏览器提供虚拟目录的别名。

下面，按照表 9.2 中的设置，练习建立物理目录和虚拟目录。

表 9.2　建立物理目录和虚拟目录

	实际存储位置	别名	URL 路径
物理目录	C:\inetpub\wwwroot\linux	Linux	http://www.xpc.cn/linux
虚拟目录	D:\xunilinux	Xunilinux	http://www.xpc.cn/xunilinux

1）物理目录创建

在网站的主目录（%systemroot/inetpub/wwwroot）下，建立一个名称为 linux 的文件夹，然后在此文件夹内建立一个名称为 default.htm 的文件，此文件内容如图 9.21 所示。

然后打开“Internet 信息服务（IIS）管理器”窗口，可以看到网站多了一个物理目录“linux”。如图 9.22 所示。

用户在客户端浏览器内利用“http://192.168.11.250/linux”连接此物理目录后，将看到如图 9.23 所示的窗口。

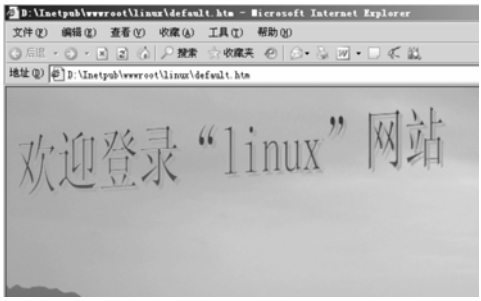

图 9.21　default.htm 内容（1）

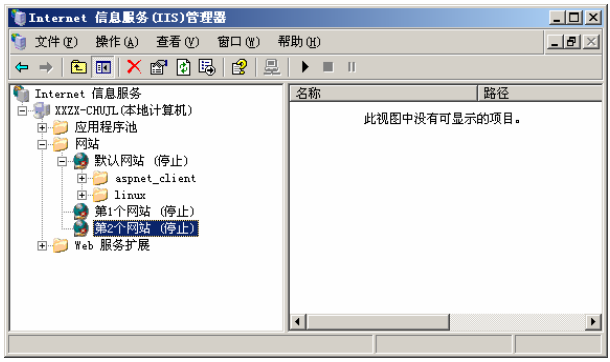

图 9.22　网站物理目录

2）虚拟目录创建

创建虚拟目录过程如下。

（1）在 D 磁盘驱动器下，建立一个名称为“xunilinux”的文件夹，然后在此文件夹内建立一个名称为“default.htm”的文件，此文件内容如图 9.24 所示。

（2）选择要在其中创建虚拟目录的 Web 站点，右击，在弹出的菜单中选择“新建→虚拟目录”选项，弹出“虚拟目录创建向导”对话框。

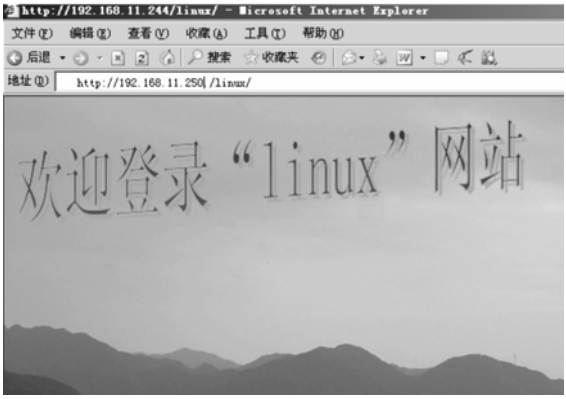

图 9.23　浏览 linux 网站

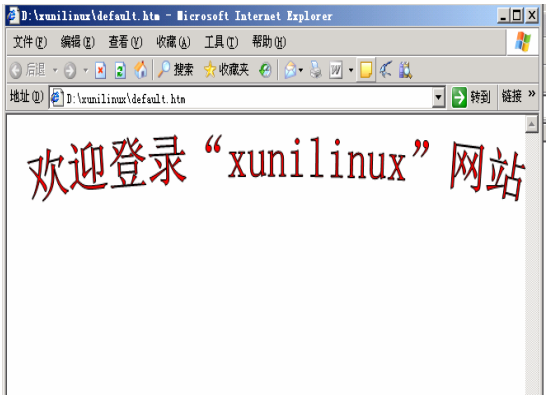

图 9.24　default.htm 内容（2）

（3）单击“下一步”按钮，弹出“虚拟目录别名”对话框。在“别名”文本框中输入“xunilinux”，如图 9.25 所示。

（4）单击“下一步”按钮，弹出“网站内容目录”对话框，在“路径”文本框中输入“D:\xunilinux”，如图 9.26 所示。

图 9.25 “虚拟目录别名”对话框

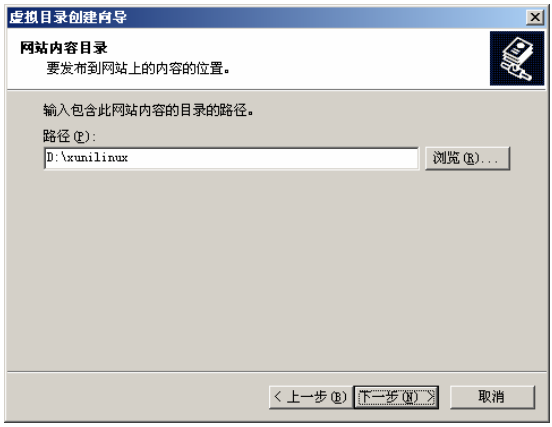

图 9.26 “网站内容目录”对话框

（5）单击“下一步”按钮，弹出“虚拟目录访问权限”对话框，在“权限”列表中选择“读取”和“运行脚本”等复选项，单击“下一步”按钮，单击“完成”按钮完成虚拟目录创建。打开“Internet 信息服务（IIS）管理器”窗口，可以看到网站多了一个虚拟目录“xunilinux”，如图 9.27 所示。

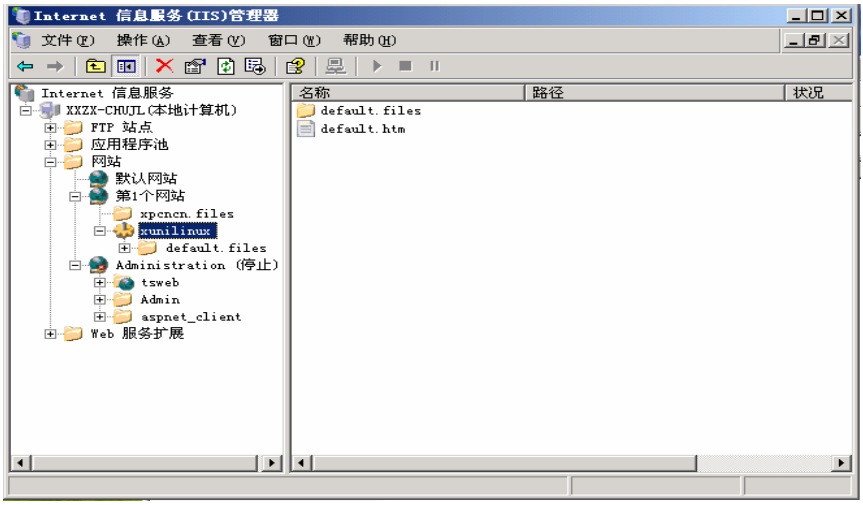

图 9.27 网站虚拟目录

（6）虚拟目录是网站的一个组成部分，其基本属性与 Web 网站属性相似。选中要设置的虚拟目录，右击 “属性”选项，打开“虚拟目录属性”对话框，可以设置和更改网站的虚拟目录，共有 5 个选项卡。其基本属性设置与 Web 网站管理类似，因为 Web 网站的主目录本身就是一个特殊的“根”虚拟目录，可以将其别名视为“ / ”。

（7）虚拟目录浏览。在客户端浏览器的地址栏中输入“http：//IP 地址/目录名”或“http：//域名/目录名”，如 http://www.xpc.cn/xunilinux，即可直接浏览建立的虚拟目录。

（8）也可以将另外一台计算机内的共享文件夹设为虚拟目录。在如图 9.28 所示的对话框中，在“路径”文本框中按照“\\计算机名或 IP 地址\共享名”格式输入，但必须输入有权访问此文件夹的用户名和密码。如图 9.29 所示。

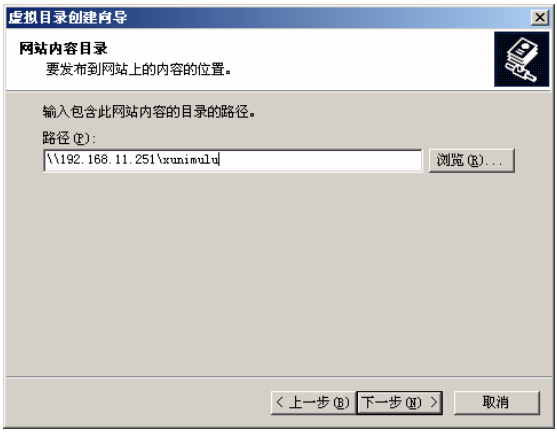

图 9.28　远程虚拟目录

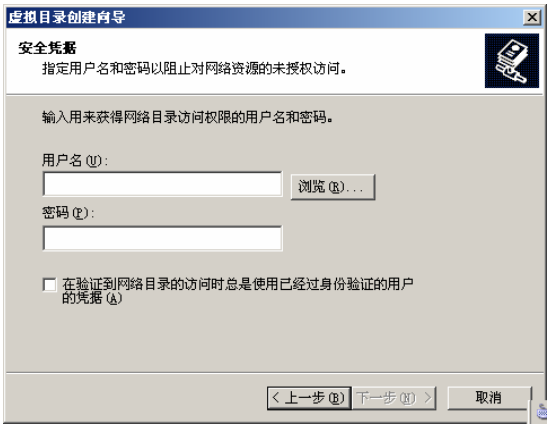

图 9.29　输入用户名和密码

步骤 8：网站的管理与维护

1）网站的启动、停止和删除

在“Internet 信息服务（IIS）管理器”窗口，单击“网站”，然后用鼠标右键单击需要管理的网站，在快捷菜单中进行选择：

- 选择“启动”命令，可以重新启动网站；
- 选择“暂停”命令，可以暂停网站；
- 选择“停止”命令，可以停止网站运行；
- 选择“删除”命令，可以将网站删除。

2）设置 Web 站点标识

在如图 9.30 所示的“xpc 网站属性”对话框中，在默认“网站”选项卡下进行 Web 站点标识设置。

（1）在“网站标识”区域，可以修改站点描述、Web 站点使用的 IP 地址、TCP 端口及 SSL 端口等信息，这些信息都是在创建 Web 站点时指定的。

（2）在“描述”栏中可以设置该 Web 站点的标识。该标识对于用户的访问没有任何意义，其作用只是当服务器中安装多个 Web 服务器时，便于网络管理员进行区分，即站点标识将作为 Web 服务器的名称显示在“Internet 信息服务（IIS）管理器”窗口目录树中。

（3）在“IP 地址”下拉列表中可以为该站选择一个 IP 地址，该 IP 地址必须是在“网络连接→本地连接”中配置给当前计算机（网卡）的 IP 地址。在这里选择“192.168.11.250”。由于 Windows Server 2003 可安装多块网卡，并且每块网卡可绑定多个 IP 地址，因此，服务器可以拥有多个 IP 地址。如果这里不分配 IP 地址，即选用“全部未分配”，则该站点将响应所有未分配给其他站点的 IP 地址，即以该计算机默认站点的身份出现。当用户向该计算机的一个 IP 地址发出连接请求时，如果该 IP 地址没有被分配给其他站点使用，将自动打开这个默认站点。

（4）在“TCP 端口”文本框中为站点指定一个 TCP 端口以运行服务，默认的端口号是 80。也可以设置其他任意一个唯一的 TCP 端口，这时需以“IP：TCP Port”的格式访问，否则将无法连接到该站点。

（5）单击“高级”按钮，显示“高级网站标识”对话框，如图 9.31 所示，在该对话框中可以为该站点添加其他的 IP 地址和端口，选中一个项目，单击“编辑”按钮可以修改站点的

主机头值。

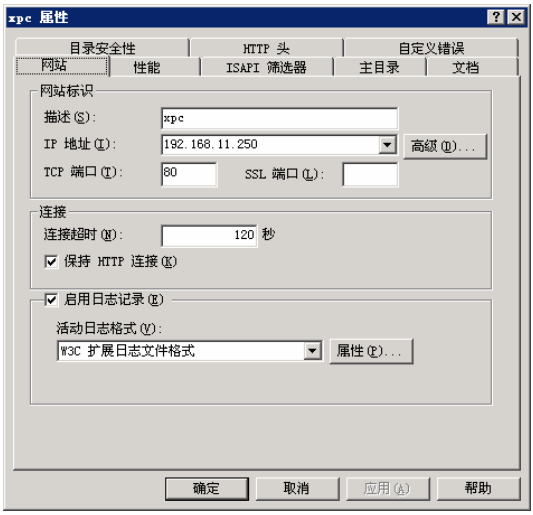

图 9.30 “XPC 属性”对话框

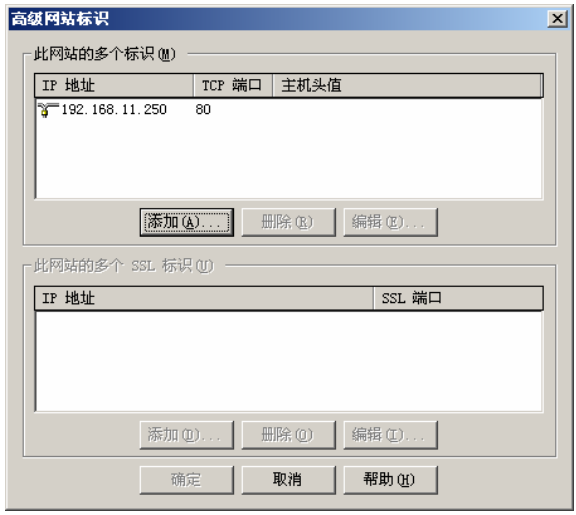

图 9.31 “高级网站标识”对话框

（6）SLL 端口：Web 服务器安全套接字层（SSL）的安全功能利用一种称为“公用密钥”的加密技术保证会话密钥在传输过程中不被截取。

要指定安全套接字层加密使用的端口，须在“SSL 端口”框中输入端口号，该端口号的默认值为“443”。

用户的 Web 浏览器在与 Web 服务器建立安全通信链接时，需要通过 https://address 方式访问，如 https://192.168.11. 250；但若将 SSL 端口指定为其他端口（非 443）时，必须指定该端口，即 https://ipaddress:port，如 https://192.168.11.250:8080。

注意 只有使用 SSL 加密时才需要 SSL 端口号。

（7）在图 9.30 的“连接”区域中，可以设置站点的连接属性，这些属性通常决定了站点的访问性能。

“连接超时”：例如默认的连接超时为 120s。如果一个连接与 Web 站点未交换信息的时间达到指定的连接超时时间，Web 站点将中断该连接。

“保持 HTTP 连接”：选择“保持 HTTP 连接”复选框能够加快网站对用户的响应速度。

3）配置 Web 站点的性能

打开“性能”选项卡，如图 9.32 所示，可以设置所选网站占用的系统带宽（网站所用的总流量）和网站连接限制（允许的并发连接数量）。如果带宽有限，选中“限制网站可以使用的网络带宽”复选框，并在“最大带宽”文本框中输入合适的数值。如果服务器性能有限，选中“网站连接”区域中的“连接限制为”单选框，并设置一个合适的数值。

4）设置主目录和目录文件权限

每个网站必须有一个主目录。主目录位于发布的网页的中央位置，包含主页或索引文件，以及到所在网站其他网页的链接。主目录是网站的“根目录”，映射为网站的域名或服务器名。用户使用不带文件名的 URL 访问 Web 网站时，请求将指向主目录。“默认 Web 站点”的主目录默认为 c:\inetpub\wwwroot。主目录是在建立过程中指定的。更改 Web 站点的主目录的方法如下。

（1）在图 9.30 所示的“xpc 属性”对话框中单击“主目录”选项卡，如图 9.33 所示。

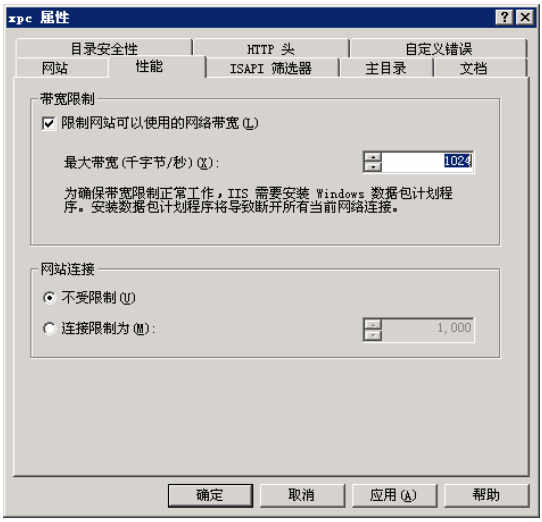

图 9.32 “性能”对话框

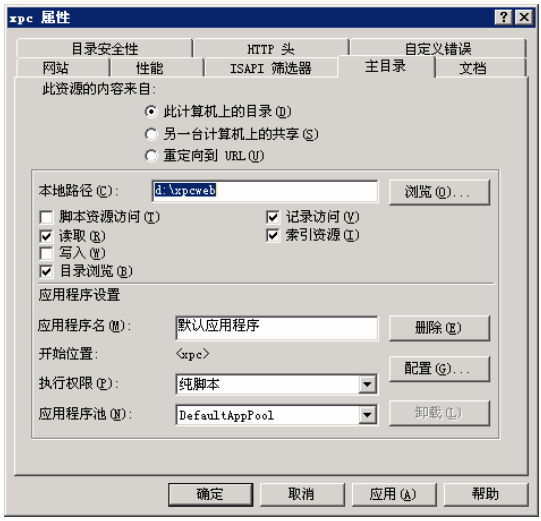

图 9.33 “主目录”对话框

（2）主目录可以来自 3 个位置：此计算机上的目录、另一台计算机上的共享和重定向到 URL。用户可以选择其中一种，这时本地路径的表示方法会随着选择位置的不同而不同。

① 选择“此计算机上的目录”单选钮：表示主目录的内容位于服务器上，在“本地路径”文本框中输入完整的目录路径（此时必须使用绝对路径），如 d:\xpcweb，即可将该 Web 网站的主目录修改至新的位置。或者单击“浏览”按钮查找所需的目录路径。

② 选择“另一台计算机上的共享”单选钮：此时“本地路径”变为“网络目录”，表示主目录的内容位于其他计算机的共享目录。在“网络目录”文本框中输入完整的 UNC 路径，格式为“\\｛服务器名｝\｛共享名｝”，如图 9.34 所示，然后单击“连接为”按钮，打开“网络目录安全凭据”对话框，设置能够访问该资源的 Windows 账户和密码。如果选中下面的复选框，系统会根据当前登录的用户名和密码来验证试图连接到远程共享的连接，不用设置用户名和密码；清除该选项之后，所有到远程共享的客户端连接都将使用输入的特定用户名和密码。

③ 选择“重定向到 URL”单选钮：如图 9.35 所示，此时“本地路径”变为“重定向到”，表示将向主目录的客户请求直接导向其他的网络资源。当浏览器访问该站点时，将自动指向“重定向到”文本框所提供的目标 URL，以便浏览器跳转到指定的 Web 页。

“上面输入的准确 URL”：表示将客户需求重定向到某个网站或目录。将虚拟目录重定向到目标 URL，但不会添加原始 URL 的任何部分。选中该选项可以将整个虚拟目录重定向到一个文件。例如，若要将对/scripts 虚拟目录的所有请求都重定向到主目录中的 default.htm 文件，可以在“重定向到”文本框中输入“/default.htm”，然后选中该选项。

“输入的 URL 下的目录”：表示父目录重定向到子目录。例如，要将主目录重定向到子目录“newhome”，应在“重定向到”文本框中输入“/newhome”，然后选中该选项。如果不选中该选项，Web 服务器会继续将父目录映射为其自身。

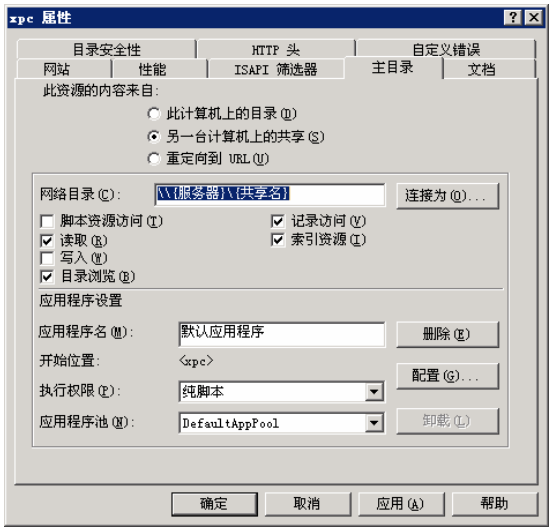

图 9.34　另一台计算机上的共享

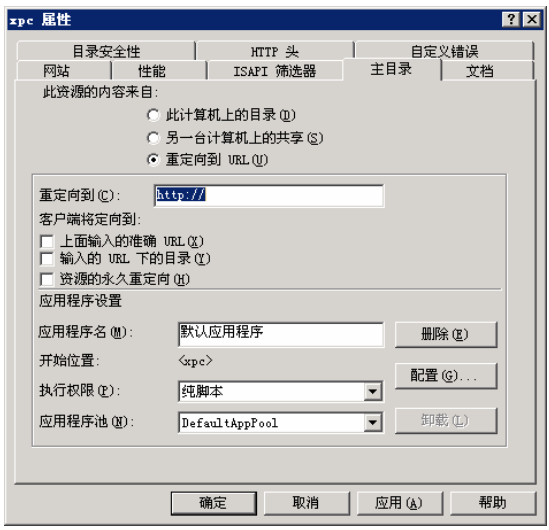

图 9.35　重定向到 URL

“资源的永久重定向”：表示将消息“301 永久重定向”发送到客户。重定向被认为是临时的，而且客户浏览器收到“302 临时重定向”。

（3）对主目录的访问控制

当将主目录指定为“此计算机上的目录”或“另一计算机上的共享位置”时，可控制用户对主目录的访问权限。如图 9.34 所示。用户对主目录的访问权限主要有以下几种。

① 脚本资源访问：若允许用户访问已经设置了“读取”或“写入”权限的资源代码，请选中该选项。当选择“脚本资源访问”权限时，用户可以从 ASP 等应用程序脚本中查看敏感信息，如用户名和密码，并可以更改在服务器上运行且对服务器安全和性能具有重要影响的源代码。

② 读取：若允许用户读取或下载文件（目录）及其相关属性，请选中该项。

③ 写入：若允许用户将文件及其相关属性上载到服务器上已启用的目录中，或者更改可写文件的内容，请选中该选项。“写入”操作只能在支持 HTTP1.1 协议标准的浏览器中进行。

④ 目录浏览：若允许用户查看该虚拟目录中文件和子目录的超文本列表，请选中该选项。需要注意的是，虚拟目录不会显示在目录列表中，因此，如果用户欲访问虚拟目录，必须知道虚拟目录的别名。如果不选择该选项，当用户试图访问文件或目录并没有指定访问其中的某个文件时，将在用户 Web 浏览中显示“禁止访问”消息；如果选中该选项，当用户直接访问该 Web 网站中的某一目录时，将显示该路径中的所有文件和目录结构。因此为了安全起见，建议不选择该选项。

⑤ 记录访问：若在日志文件中记录对该目录的访问，请选中该选项。只有启用该 Web 站点的日志记录时才会记录访问。

⑥ 索引资源：若允许 Microsoft Indexing Services 将该目录包含在 Web 站点的全文本索引中，请选中该选项。

5）自定义错误信息

每一个网站都应为自己的用户提供出错信息。HTTP 协议提供了一系列标准的错误代码，

分别指示出错原因及错误对象、可能的处理方法等信息。例如，404 错误代表客户机请求的文件不存在；401.2 错误代表客户没有相应权限访问指定资源。

自定义错误信息的方法如下：

① 在“默认网站属性”对话框中单击“自定义错误信息”选项卡，弹出“自定义错误信息”对话框，列出各种 HTTP 错误类型。

② 选择需要自定义的错误类型，单击“编辑属性”按钮。弹出“编辑自定义错误属性”对话框，如图 9.36 所示。在“消息类型”下拉列表中指定“默认”，可以使用默认的错误信息；指定“文件”，并单击“浏览”可以将自定义的.htm 文件作为该类型错误的信息指示文件。

③ 还有一种方式是在“消息类型”下拉列表中指定“URL”，并在“URL”栏中指定一个网页作为出错误信息指示文件。使用 URL 方式时，必须保证所指定的 URL 位于本地服务器上。

6）设置内容自动失效和 HTTP 头

网站中的某些信息是对时间敏感的，如专门报价或通知公告，过期之后它们将失去存在价值。它为当前主页预先定义过期时限，浏览器在加载网页时将当前日期与失效日期进行比较，以便确定是显示高速缓存页还是从服务器请求更新主页。

（1）设置内容自动失效。设置内容自动失效的方法如下。

① 在“默认网站属性”对话框中单击“HTTP 头”选项卡，如图 9.37 所示。

② 选择“启用内容过期”复选框。

③ 指定过期方式，可选的方式有 3 种。

图 9.36 “编辑自定义错误属性”对话框

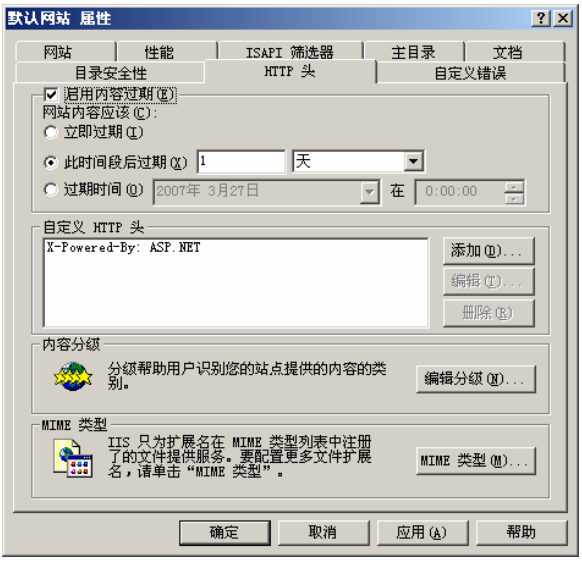

图 9.37 “HTTP 头”对话框

- 立即过期：当浏览器下次请求该网页时，将下载该网页的新版本，永远不会从客户端的缓存中加载该网页。其结果是每次访问该页时，都需要重新从 Web 站点下载该页。
- 此时间段后过期：指定若干时间以后网站内容过期。在该时间段结束之前，将从缓存中检索网页，而无须再从 Web 站点下载，从而提高了浏览速度。只有时间过期后，浏览器才从 Web 站点重新下载该页。

➢ 过期时间：指定失效的具体日期和时间。在这一时间到来之前，客户端将从缓存中检索网页，只有时间过期后，浏览器才从 Web 站点重新下载该页。

根据实际需要选择过期方式。例如，指定网页下载 3 天后过期，则选择“此时间段后过期”，然后选择数量 3，单位天。

④ 单击“应用”按钮、“确定”按钮完成。

（2）自定义 HTTP 头。自定义 HTTP 头可用来发送当前 HTML 规范中尚不支持的指令，如产品发布时 IIS 尚不支持的更新的 HTML 标签。例如，可以使用自定义的 HTTP 头允许客户浏览器高速缓存页，但却可以防止代理服务器高速缓存该页。

单击“自定义 HTTP 头”栏右侧的“添加”按钮，打开“添加/编辑自定义 HTTP 头”对话框，输入自定义 HTTP 头的名称及其值。单击“确定”按钮返回。该自定义的 HTTP 头将从 Web 服务器发送到客户浏览器。

（3）内容分级。分级设置主要是通过对网站的内容进行分级，防止不具备等级要求的其他访问者查看站点内容。通过分级设置，当用户访问网页时，浏览器会根据分级设置和站点的分级要求来决定哪些内容可以浏览，哪些内容不可以浏览。

Windows Server 2003 提供暴力、性、裸体和语言 4 个分级设置。

① 在图 9.37“HTTP 头”窗口中单击 “编辑分级”按钮，弹出“内容分级”对话框，如图 9.38 所示。选中“对此内容启用分级”复选项，在“类别”列表框中，依次选择暴力、性、裸体和语言 4 个类别之一，调节分级滑块，改变所选类别的分级级别。

② 如果需要，可以设置内容分级人员的电子邮件地址和内容分级的过期时间。完成设置后，单击“确定”按钮返回到“默认 Web 站点属性”窗口，再单击“确定”按钮，保存设置。

7）指定网站管理员

每一个网站都有一位管理员，负责本网站的管理工作。同一台 Web 服务器上的管理员只能访问他所负责的网站，而不能访问其他的网站。为网站指定管理员的方法如下：

（1）在打开的“Internet 信息服务（IIS）管理器”窗口中，选择要指定管理员的网站，右击鼠标并在弹出菜单中选择“权限”选项，进入“安全”对话框，如图 9.39 所示。

（2）从“组或用户名称” 列表中删除不允许访问网站的用户名，保留或增加用于管理网站的用户名。

步骤 9：启用和停用动态属性

为了更好地预防恶意用户和攻击者的攻击，在默认情况下，IIS 服务在高度安全和“锁定”的模式下安装。因此，默认情况下，IIS 只为静态 HTML 内容提供服务，这意味着 Active Server Pages（ASP）、ASP.net、索引服务、在服务器端的包含文件（SSI）、Web 分布式创作和版本控制（WebDAV）、FrontPage Server Extensions 等功能将不会工作，除非启用它们。如果在未启用这些功能前使用 IIS 的这些功能，IIS 将返回错误信息，所以，应该在安装 IIS 6.0 后启用所需的服务。

只有本地计算机上 Administrators 组的成员或者被委派了相应的权限的用户，才能执行启用服务扩展任务。

要使 IIS 支持动态网页，必须启动服务器端的 ASP，ASP.net 文件，WebWAV 发布和 FrontPage Server Extensions 等服务扩展。

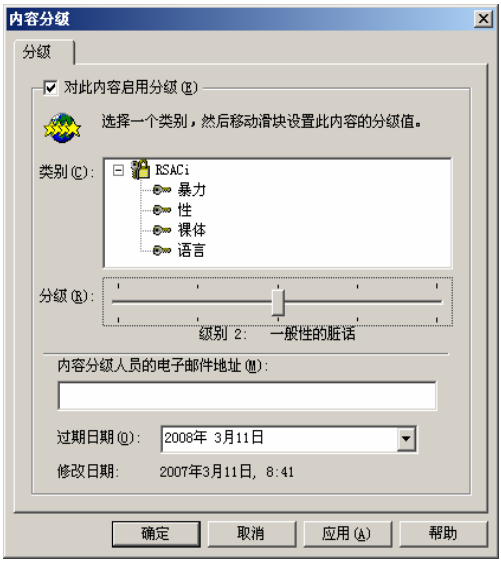

图 9.38 “内容分级”对话框

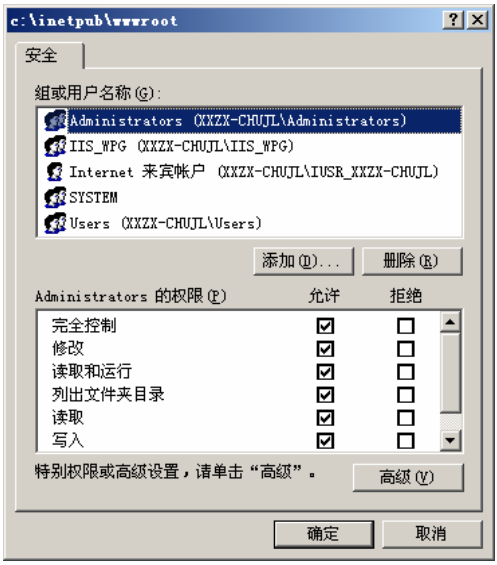

图 9.39 “安全”对话框

1）启用和禁用 Web 服务扩展

（1）在“Internet 信息服务（IIS）管理器”窗口，展开本地计算机，单击“Web 服务扩展”文件夹。

（2）在右边详细信息窗格中，选择要启用或禁用的“Web 服务扩展”，如图 9.40 所示。

图 9.40 Web 服务扩展

- 启用已禁用的 Web 服务扩展，单击“允许”按钮；
- 禁用已启用的 Web 服务扩展，单击“禁止”按钮；
- 查看 Web 服务扩展的属性，单击“属性”按钮。

（3）单击“确定”按钮即可。

2）允许应用程序调用 Web 服务扩展

允许指定应用程序调用 Web 服务扩展，操作步骤如下：

（1）在“Internet 信息服务（IIS）管理器”窗口，展开本地计算机，单击“Web 服务扩

展”文件夹。

（2）在右边详细信息窗格中，单击“对特定的应用程序允许所有 Web 服务扩展”超链接，打开“对特定的应用程序允许所有 Web 服务扩展”对话框，从“应用程序”下拉列表框中选择应用程序的名称，如图 9.41 所示。在“要允许的扩展”框中将出现允许应用程序调用的 Web 服务扩展，单击“确定”按钮即可。

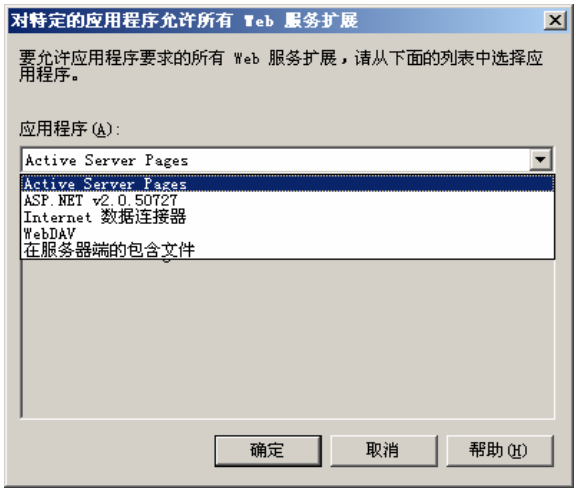

图 9.41　对特定的应用程序允许所有 Web 服务扩展

3）禁用所有 Web 服务扩展

（1）在“Internet 信息服务（IIS）管理器”窗口，展开本地计算机，单击“Web 服务扩展”文件夹。

（2）在右边详细信息窗格中，单击“禁用所有 Web 服务扩展”超链接，将出现一条警示消息。如图 9.42 所示。

图 9.42　禁用所有 Web 服务扩展

- 要禁用所有扩展，单击“是”按钮；
- 要取消操作，单击“否”按钮；
- 要查看详细信息，单击“帮助”按钮。

（3）如果单击“是”按钮，每个 Web 服务扩展的状态都将变成禁止。

步骤 10：IIS 6.0 的网站安全

Web 服务器的功能越多，采用的技术越复杂，其潜在的危险性就越大。Web 安全涉及的因素多，必须从整体安全的角度来解决 Web 安全问题，实现物理级、系统级、网络级和应用级的安全。

1）IIS 6.0 的安全机制

严格地说，IIS 6.0 本身提供的是一种应用级的安全机制，它以 Windows Server 2003 操作系统和 NTFS 文件系统的安全性为基础，提供了强大的安全管理和控制功能。

如果 Web 站点的内容位于 Windows Server 2003 的 NTFS 分区，则可以通过 4 种方法限制用户访问 Web 站点提供的资源。它们之间的关系如图 9.43 所示。

（1）IP 地址限制：通过 IP 地址来限制或允许特定的计算机（组）或整个网络访问 Web 站点中的资源。当用户访问 Web 站点时，Web 站点将审核用户计算机的 IP 地址，以决定是否允许其访问 Web 站点中的资源。

（2）用户验证：对于 Web 站点中的一般资源，可以采用匿名访问，而对于一些特殊资源则需要有效的 Windows Server 2003 用户登录。

（3）Web 权限：Web 站点的操作员可以为站点、目录和文件设置权限，如读、写或执行。这些权限适用于所有的用户。

（4）NTFS 权限：如果 Web 站点的内容位于 NTFS 分区，可以借助于 NTFS 的目录和文件权限来限制用户对站点内容的访问，如完全访问、拒绝访问、读取、更改等权限。

设置 IIS 的安全性功能是在“目录安全性”选项卡中进行的，用于在授权访问受限制的内容之前确认用户的身份标识。其中包括 3 项：身份验证和访问控制，IP 地址和域名限制，安全通信。如图 9.44 所示。

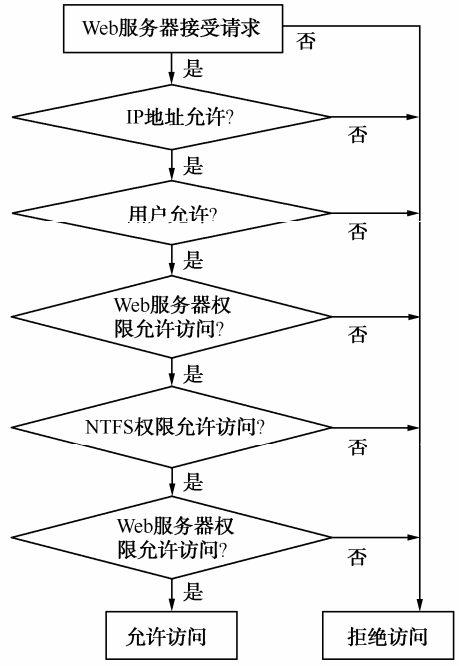

图 9.43　关系图

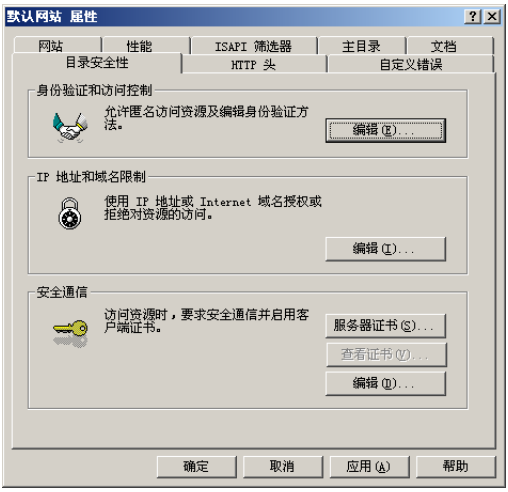

图 9.44　“目录安全性”对话框

2）通过 IP 地址限制保护网站

当用户首次尝试访问 Web 网站的内容时，IIS 将会检查每个来自客户端的接收报文的源 IP 地址，并将其与网站设置的 IP 地址进行比较，以决定是否允许该用户访问。IP 地址及域名限制是指通过适当的配置，即可允许或拒绝特定计算机、计算机组或域访问 Web 站点、目

录或文件。例如，可以防止 Internet 用户访问 Web 服务器，方法是仅授予 Internet 成员访问权限而明确拒绝外部用户的访问。限制 IP 地址和域名的方法如下。

（1）在图 9.44 所示的“目录安全性”对话框中，单击“IP 地址和域名限制”区域中的“编辑”按钮，弹出“IP 地址和域名限制”对话框，如图 9.45 所示。通过下列两种方式限制 IP 地址的访问。

- 选择“授权访问”单选按钮，则除了“下列除外”列表框中的计算机外，其他所有的计算机都可访问该 Web 服务器上的内容，即默认地允许所有的计算机访问 Web 站点。如果要限制某些计算机访问该 Web 站点，单击“添加”按钮，在“下列除外”列表中加入所限制访问的计算机。这种方式适用于仅拒绝少量用户访问的情况。
- 选择“拒绝访问”单选按钮，则除了“下列除外”列表框中的计算机外，其他所有的计算机都不能访问该 Web 服务器上的内容，即默认限制所有的计算机访问 Web 站点。如果要允许某些计算机访问该 Web 站点，单击“添加”按钮，在“下列除外”列表中加入所允许访问的计算机。这种方式适用于仅授予少量用户访问权限的情况。

（2）选择一种限制方式后，如选择“授权访问”单选按钮，单击“添加”按钮，打开“拒绝访问”对话框，如图 9.46 所示。

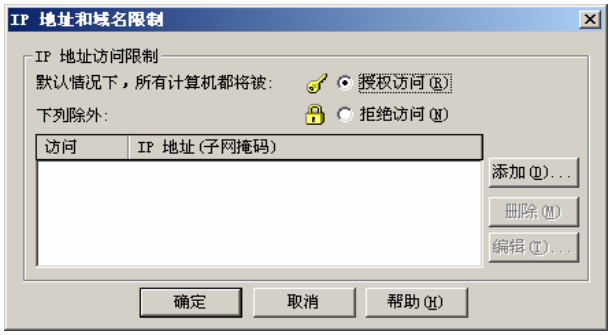

图 9.45 “IP 地址和域名限制”对话框

图 9.46 “拒绝访问”对话框

有 3 种类型用于限制 IP 地址：

- 一台计算机：需要在“IP 地址”文本框中输入要拒绝的计算机的 IP 地址；也可以通过单击“DNS 查找”按钮，查找 DNS 域中的计算机。
- 一组计算机：需要在“网络标识”文本框中输入要授权的一组计算机中的任何一台计算机的 IP 地址，并在“子网掩码”文本框中输入子网掩码，如图 9.47 所示。
- 域名：需要在“域名”文本框中输入授权域的域名，如图 9.48 所示。

（3）单击“确定”按钮返回 “IP 地址和域名限制”对话框，再单击“确定”按钮，完成设置。

这样，被添加的单台计算机、一组计算机或者一个域的客户就不能访问服务器，而其他的客户则有访问权。

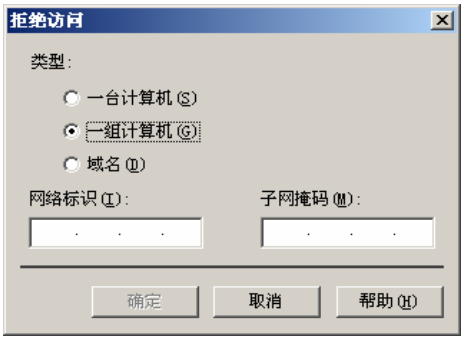

图 9.47 “一组计算机”限制

图 9.48 “域名”限制

3）通过身份验证控制特定用户访问网站

“身份验证和访问控制”选项组允许配置 Web 服务器，是其在指派受限内容的访问权限之前确认用户的身份标识。但是，必须先创建有效的 Windows 用户账户，然后配置这些账户的 NTFS 目录和文件访问权限，Web 服务器才能验证用户的身份。如果创建的 Web 站点只在局域网内使用，并且只允许授权用户访问，则在“身份验证方法”对话框选择默认值；如果创建的 Web 站点允许匿名用户访问，或者允许 Internet 上的用户访问，则撤销“集成 Windows 身份验证”复选框。

设置匿名访问的方法如下。

（1）在图 9.44 所示的“目录安全性”对话框中，单击“身份验证和访问控制”区域中的“编辑”按钮，弹出“身份验证方法”对话框，如图 9.49 所示。选中“启用匿名访问”复选项。默认的匿名账户由字母“IUSR”和计算机名组成。

（2）启用匿名账户后，就可以更改用户匿名请求的用户账户和密码。在“用户名”文本框中输入用户账户或者单击“浏览”按钮，弹出“选择用户”对话框，如图 9.50 所示，选择一个现有的 Windows 用户账户。

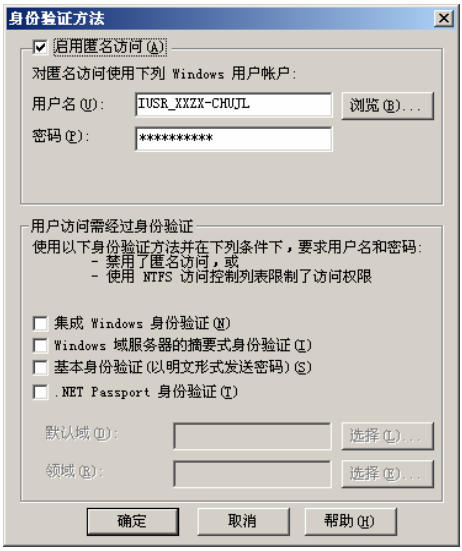

图 9.49 “身份验证方法”对话框

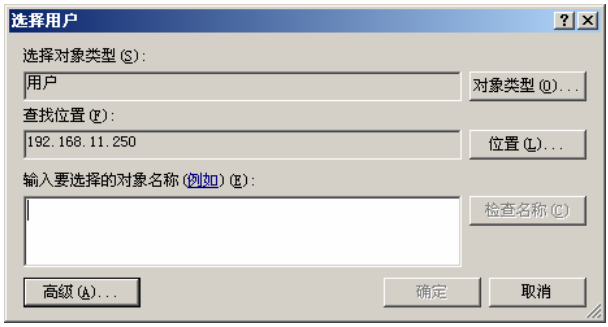

图 9.50 “选择用户”对话框

（3）多次单击“确定”按钮，完成匿名访问设置。

4）使用网站权限保护 Web 网站

网站权限适用于所有访问网站的用户，又称“Web 服务器权限”或“Web 权限”。可以针对整个网站、目录和文件夹设置网站权限，这些权限适用于所有的用户，无论它们是否拥有特定的访问权限。

如果禁用 Web 服务器权限（如读取），将限制所有用户（包括拥有 NTFS 高级别权限的用户）访问网站。如果启用了读取权限，则允许所有用户查看文件，除非通过 NTFS 权限来限制某些用户或组的访问权限。

在设置网站或虚拟目录的安全属性时，Web 服务器将提示用户是否具有重新设置单独的目录和文件属性的权限。如果选择重新设置这些属性，那么之前设置的安全属性将由新的设置替代。

要为 Web 内容设置 Web 服务器权限，可在 IIS 服务器中选择 Web 网站、虚拟目录或文件，右击“属性”，打开“属性设置”对话框，设置读取、写入、脚本资源访问、目录浏览、日志访问、索引此资源等多种访问权限。从安全角度考虑，一般不启用写入和脚本资源访问两种权限。

5）设置目录或文件的 NTFS 权限

IIS 利用 NTFS 文件系统的安全特性为特定用户设置 Web 服务器目录和文件的访问权限，也可以配置给某个用户或组授予的服务器文件和目录访问级别。例如，可以将 Web 服务器上的某个文件配置为允许某用户查看和执行，而禁止其他用户访问该文件。

NTFS 权限在项目 3 中已经介绍过，在这里不再介绍。要使用 NTFS 权限保护目录或文件必须具备以下两个条件：

（1）要设置权限的目录或文件必须位于 NTFS 分区中。

（2）对于要授予权限的用户或用户组，应设立有效地 Windows 账户。在 Windows Server 2003 中，可以在“计算机管理”控制台中创建 Windows 用户账户或组。

NTFS 权限可在资源管理器中设置，也可直接在 IIS 管理器中设置。在 IIS 管理器中右击某个网站或文件，选择“权限”命令，打开“安全”对话框，如图 9.51 所示，在“组或用户名称”列表框中查看对当前目录设置权限的组或用户，可根据需要添加或删除组或用户，也可直接编辑修改某一用户的权限。要允许或拒绝某一权限，应在“组或用户的权限”列表框中选中“允许”或“拒绝”复选框。

如果要为组或用户设置特殊权限，则单击“高级”按钮，打开“高级安全设置”对话框，如图 9.52 所示，查看或更改现有组或用户的特殊权限。

6）审核 IIS 日志记录

日志是以文件形式监视网站使用情况的手段。选中“启用日志记录”复选框，然后在“活动日志类型”下拉列表框中指定日志类型，各种日志类型的内在差别并不是很大，常用的日志类型有以下 4 种：

- “Microsoft IIS 日志文件格式”是一种固定的 ASCII 格式；
- “NCSA 公用日志文件格式”是一种固定的 ASCII 格式，它是国家超级计算应用中心的公用格式；
- “W3C 扩展日志文件格式”是一种可以自行定制的格式；
- “ODBC 日志记录”将记录保存到数据库。

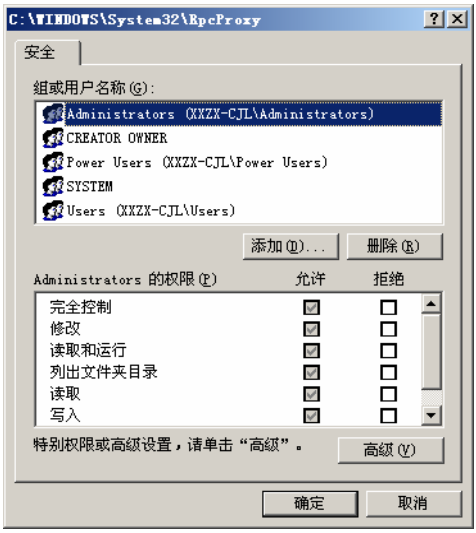

图 9.51 “安全”对话框

图 9.52 “高级安全设置”对话框

选用一种格式（默认格式是 W3C 扩展日志文件格式）后，单击“属性”按钮可以对日志进行设置。

选定日志文件类型后，单击“属性”按钮，打开如图 9.53 所示的“日志记录属性”对话框。“常规”标签提供了一般性的日志文件设置界面。可以在“日志文件目录”框中更改日志文件存储的路径。日志是一种持续性的记录手段，随着时间的推移，单个日志文件所记录的事件越来越多，也越来越大。为了防止日志文件太大所导致的存储及分析困难，应该在日志文件达到一定大小的时候新建一个文件。通常的判断方法有两种：一定时间后新建文件和达到一定大小后新建文件。对于前者，只需选择“每小时”、“每天”、“每周”或“每月”即可在指定时间到达时自动生成新的日志文件，新文件将以时间命名，例如 yymmdd.log 或 mmdd.log。而选择“当文件大小达到”并指定大小后，系统就可以在日志文件达到指定大小后生成新文件，默认情况下，每达到 20 MB 就要生成一个新文件。

在图 9.53 中单击“高级”标签，弹出“日志记录属性高级”对话框，如图 9.54 所示。可以指定日志文件记录何种事件及相关对象的细节，只需选取相应对象前面的复选框即可。例如，如果需要记录客户访问站点内容所使用的服务器端口号，就应选择“服务器端口”前面的复选框。

9.5 扩展知识及任务训练——虚拟主机技术

IIS 支持在一台计算机上同时建立多个网站的功能。例如，若要建立 3 个网站 www.xpc. cn、www.xpc.com、www.xpc.net，只需要一台计算机即可，不需要用到 3 台计算机，也就是在一台服务器能宿主多个网站，这就是常说的虚拟主机技术。

虚拟主机技术是使用特殊的软件技术，将一台运行在 Internet 上的服务器主机划分成若干台虚拟的主机，每一台虚拟主机都具有独立的域名，具有完整的 Internet 服务器功能，虚拟主机之间完全独立，并可由用户自行管理（一般通过 FTP 软件来进行虚拟服务器管理）。在外界看来，每一台虚拟主机和一台独立的主机完全一样。

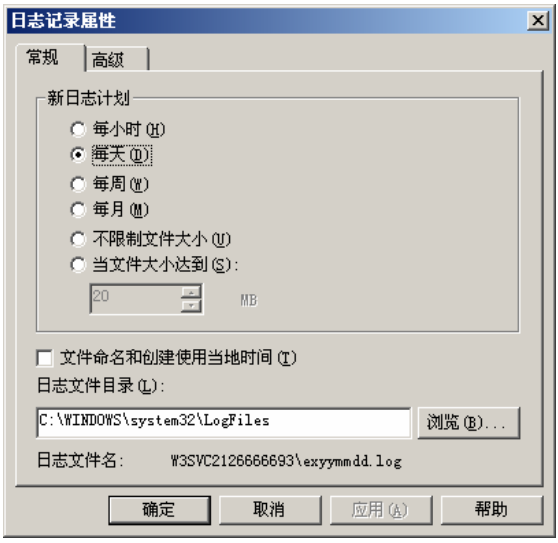

图 9.53　日志记录属性“常规”标签

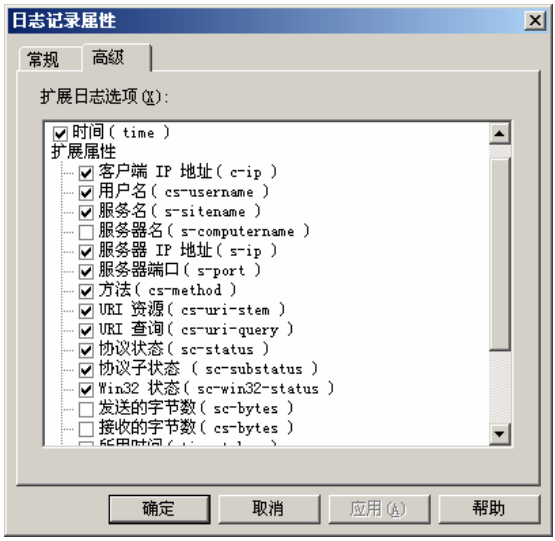

图 9.54　日志记录属性高级

虽然多个网站可以建立在同一台计算机上，但是为了让用户能够连接到正确的网站，必须给予每一个网站一个唯一的辨识身份。IIS 6.0 通过分配主机头名称、唯一的 IP 地址和 TCP 端口号来运行多个网站。每个网站都具有唯一的由端口号、IP 地址和主机头名 3 个部分组成的网站标识，用来接收和响应来自客户端的请求。通过更改其中的任何一个标识，就可在一台计算机上维护多个网站。

9.5.1　利用主机头名称建立多个网站

利用主机头名称来建立网站：当这台计算机只需要 1 个 IP 地址，就可以架设多个网站。IIS 利用主机头名称来区别每一个网站。从客户的角度看，他们只拥有自己的独立域名，而没有独立的 IP 地址，需要与他人共用一个 IP 地址，这时就不能直接通过 IP 地址进行访问。在大部分情况下，建议使用这种方法。

利用主机头名称来建立 www.xpc.cn、www.xpc.com、 www.xpc.net 三个网站，其设置见表 9.3。

表 9.3　利用主机头名称建立网站的设置

网站名称与主机头名称	IP 地址	主目录
www.xpc.cn	192.168.11.250	D:\xpcncn
www.xpc.com	192.168.11.250	D:\xpccom
www.xpc.net	192.168.11.250	D:\xpcnnet

1．将网站名称与IP地址注册到DNS服务器

在 DNS 服务器上，新建 xpc.cn、xpc.com、xpc.net 三个区域，并分别添加主机。如图 9.55 所示。

2．建立主目录

在 D 盘下，建立一个名称为 xpcncn 的文件夹，作为网站 www.xpc.cn 的主目录；建立一个名称为 xpccom 的文件夹，作为网站 www.xpc.com 的主目录；建立一个名称为 xpcnnet 的

文件夹，作为网站 www.xpc.net 的主目录。并分别在每一个文件夹下建立 default.htm 文件，作为该文件夹所对应网站的首页。

3．建立新网站www.xpc.cn

在完成上述步骤后，接下来添加 www.xpc.cn 网站。

（1）选择“开始→管理工具→Internet 信息服务（IIS）管理器”命令，打开“Internet 信息服务（IIS）管理器”窗口，鼠标右击“Internet 信息服务”树下的“网站”选项，在弹出的菜单中选择“新建→网站”选项，如图 9.56 所示。弹出“网站创建向导”对话框。

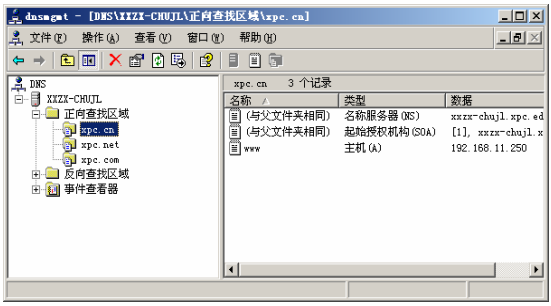

图 9.55　DNS 配置

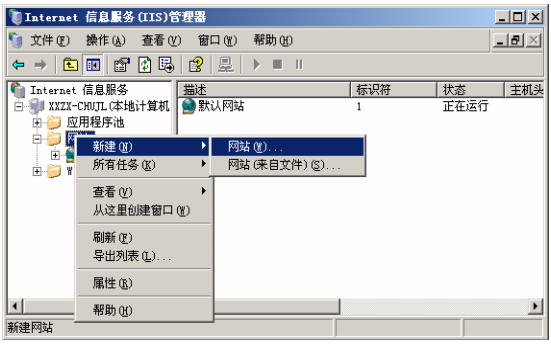

图 9.56　新建网站

（2）单击“下一步”按钮，弹出“网站描述”对话框，在“描述”栏中输入“第 1 个网站”。如图 9.57 所示。单击“下一步”按钮，弹出“IP 地址和端口设置”对话框，在“网站 IP 地址”下拉列表框中选择 IP 地址为“192.168.11.250”，在“此网站的主机头”框中输入“www.xpc.cn”。如图 9.58 所示。

图 9.57　“网站描述”对话框

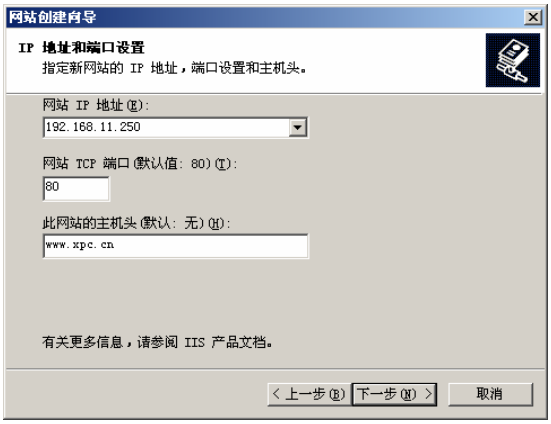

图 9.58　“IP 地址和端口设置”对话框

（3）单击“下一步”按钮，弹出“网站主目录”对话框，在“路径”框中输入“D:\xpcncn”或通过单击“浏览”按钮选择。如图 9.59 所示。

（4）单击“下一步”按钮，弹出“网站访问权限”对话框，默认选择即可。如图 9.60 所示。

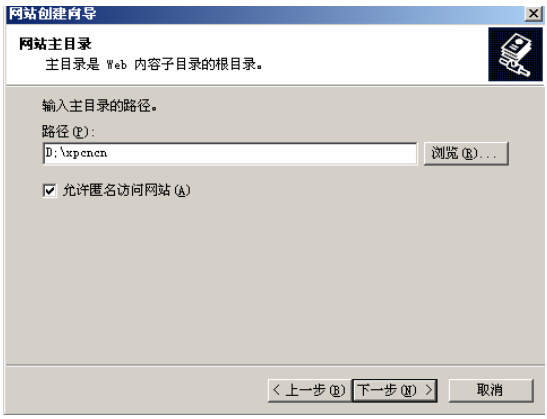

图 9.59 “网站主目录”对话框

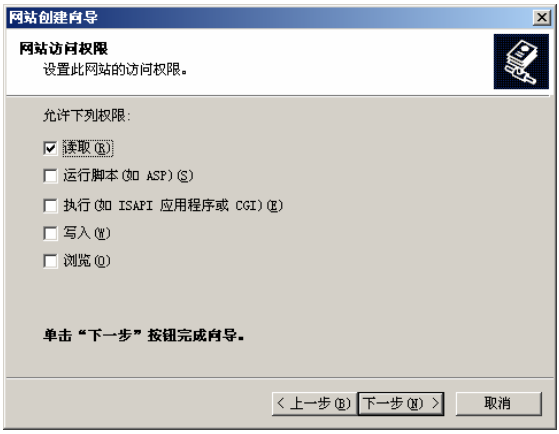

图 9.60 “网站访问权限”对话框

（5）单击“下一步”按钮，完成设置。

4．修改主机头名称

如果要修改网站的主机头名称，可以右击网站，选择“属性”选项，单击“网站标识”栏中的“高级”按钮，弹出“高级网站标识”对话框，选择一个标识，单击“编辑”按钮，弹出“添加/编辑网站标识”对话框，在“主机头值”框中修改主机头名称。如图 9.61 所示。

图 9.61 修改主机头名称

5．建立新网站www.xpc.com和www.xpc.net

按照建立新网站 www.xpc.cn 的方法建立新网站 www.xpc.com 和 www.xpc.net，注意将其主机头名称分别改为 www.xpc.com 和 www.xpc.net，主目录分别设为 D:\xpcncom 和 D:\xpcnnet。

完成后的“Internet 信息服务（IIS）管理器”窗口如图 9.62 所示。

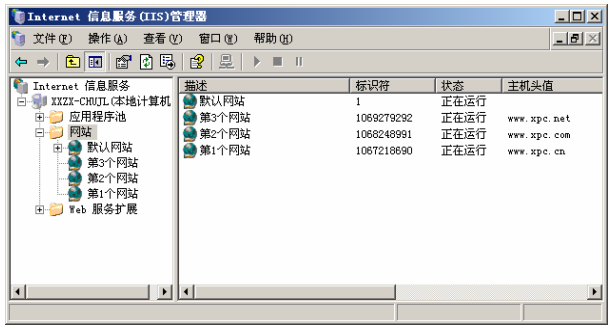

图 9.62 “Internet 信息服务（IIS）管理器”窗口

6．利用浏览器来连接新网站

用户在浏览器内利用 http://www.xpc.cn 来连接网站时，其传送到 IIS 计算机的数据包内除了包含 IIS 计算机的 IP 地址之外，还包含网址（主机头名称）www.xpc.cn，因此 IIS 计算机便可得知用户所要连接的网站为 www.xpc.cn，所以用户会看到如图 9.63 所示的画面。

同样，用户利用 http://www.xpc.com 来连接网站时看到的是如图 9.64 所示的画面。

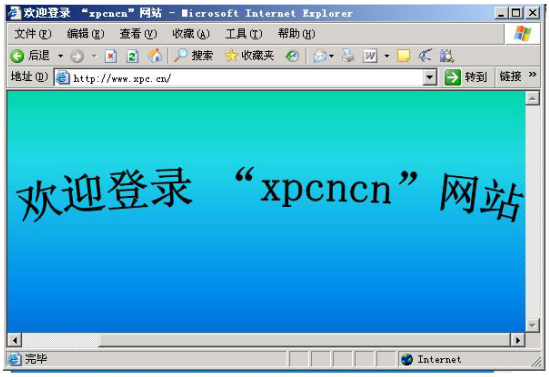

图 9.63 www.xpc.cn 网站

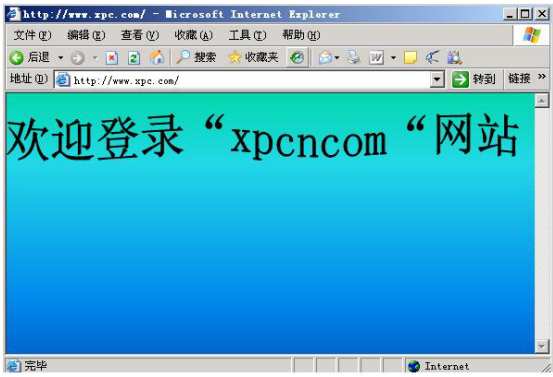

图 9.64 www.xpc.com 网站

同理，用户利用 http://www.xpc.net 来连接网站时看到的是如图 9.65 所示的画面。

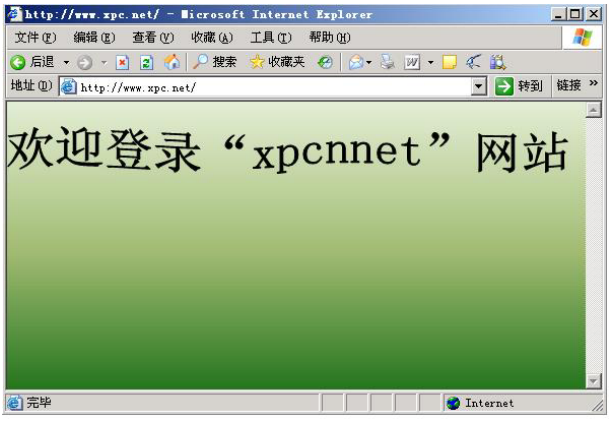

图 9.65 www.xpc.net 网站

9.5.2　利用多个IP地址建立多个网站

利用多个 IP 地址建立多个网站：此时每一个网站需要一个唯一的 IP 地址，必须将主机名称与对应的 IP 地址全部登记在 DNS 中，以后客户端只要在浏览器中输入名称，就可以连上 Web 站点。适合于对外部用户提供服务的商业网站。

利用 IP 地址建立 www.xpc.cn、www.xpc.com、www.xpc.net 三个网站，其设置见表 9.4。

表 9.4　利用 IP 地址建立网站的设置

网站名称	IP 地址	主目录
www.xpc.cn	192.168.11.250	D:\xpcncn
www.xpc.com	192.168.11.252	D:\xpccom
www.xpc.net	192.168.11.251	D:\xpcnnet

1．为计算机添加IP地址

为这台安装了 IIS 的计算机添加 3 个 IP 地址：192.168.11.250、192.168.11.251、192.168.11.252。可选择“开始→控制面板→网络连接→本地连接→属性→Internet 协议（TCP/IP）→属性高级”命令，单击“IP 地址”后面的“添加”按钮进行添加，如图 9.66 所示。

2．将网站名称与IP地址注册到DNS服务器

在 DNS 服务器上，新建 xpc.cn、xpc.com、xpc.net 3 个区域，并分别添加主机。

3．建立主目录

在 D 盘下，建立一个名称为 xpcncn 的文件夹，以作为网站 www.xpc.cn 的主目录；建立一个名称为 xpccom 的文件夹，以作为网站 www.xpc.com 的主目录；建立一个名称为 xpcnnet 的文件夹，以作为网站 www.xpc.net 的主目录。

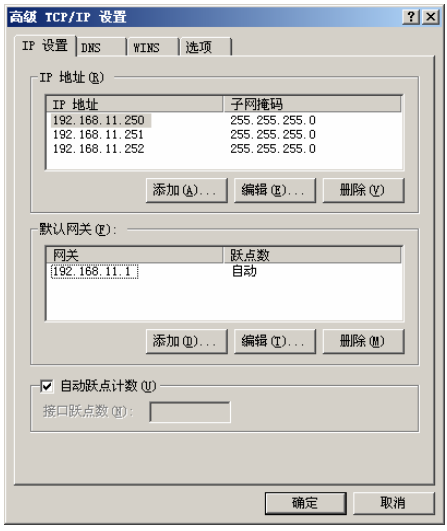

图 9.66　高级 TCP/IP 设置

4．建立新网站www.xpc.cn

在完成上述步骤后，接下来添加 www.xpc.cn 网站。

（1）选择“开始→管理工具→Internet 信息服务（IIS）管理器”命令，打开“Internet 信息服务（IIS）管理器”窗口，右击“Internet 信息服务”树下“网站”选项，在弹出的菜单中选择“新建→网站”选项，弹出“网站创建向导”对话框。

（2）单击“下一步”按钮，弹出“网站描述”对话框，在“描述”栏中输入“第 1 个网站”。单击“下一步”按钮，弹出“IP 地址和端口设置”对话框，在“网站 IP 地址”下拉列表框中选择 IP 地址为“192.168.11.250”，如图 9.67 所示。

（3）单击“下一步”按钮，弹出“网站主目录”对话框，在“路径”框中输入“D:\xpcncn”或通过单击“浏览”按钮选择。

（4）单击“下一步”按钮，弹出“网站访问权限”对话框，默认选择即可。

（5）单击“下一步”按钮，完成设置。

5．修改IP地址

如果要修改网站的 IP 地址，可以右击网站，选择“属性”选项，在“IP 地址”下拉列表框中选择 IP 地址。如图 9.68 所示。

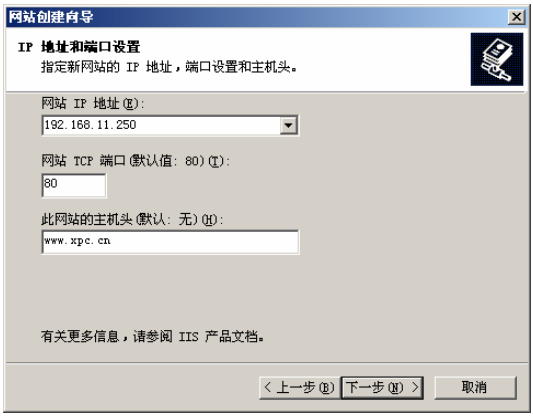

图 9.67　“IP 地址和端口设置”对话框

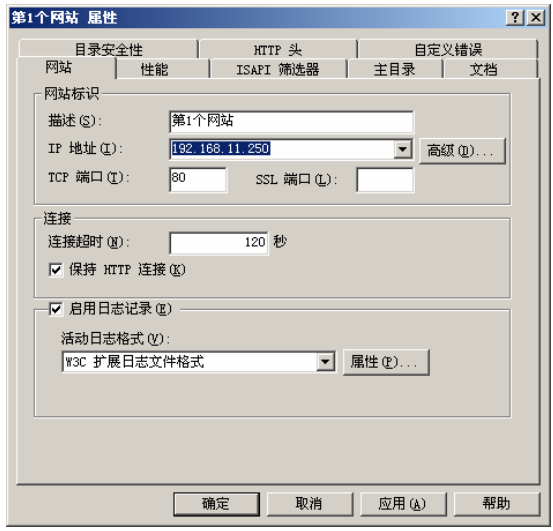

图 9.68　修改 IP 地址

6．建立新网站www.xpc.com和www.xpc.net

按照建立新网站 www.xpc.cn 的方法建立新网站 www.xpc.com 和 www.xpc.net，注意将其 IP 地址分别改为 192.168.11.251 和 192.168.11.252，主目录分别设为 D:\xpcncom 和 D:\xpcnnet。

7．利用浏览器来连接新网站

用户在浏览器内利用 http://www.xpc.cn 来连接网站时，由于 www.xpc.cn 的 IP 地址为 192.168.11.250，因此 IIS 计算机便可得知用户所要连接的网站为 www.xpc.cn。

同理，用户利用 http://www.xpc.com 和 http://www.xpc.net 来连接网站时会连接到 192.168.11.251 和 192.168.11.252。

9.5.3　利用TCP连接端口建立多个网站

利用 TCP 连接端口建立多个网站：此时每一个网站将被赋予一个非标准的 TCP 端口号，以便让 IIS 利用端口号来区别每一个网站。不建议使用此种方法。

利用 TCP 连接端口建立 www.xpc.cn、www.xpc.com、www.xpc.net 三个网站，其设置见表 9.5。

表 9.5　利用 TCP 连接端口建立网站的设置

网站名称	TCP 端口号	IP 地址	主目录
www.xpc.cn	80	192.168.11.250	D:\xpcncn
www.xpc.com	8090	192.168.11.250	D:\xpcncom
www.xpc.net	8080	192.168.11.250	D:\xpcnnet

1．将网站名称与IP地址注册到DNS服务器

在 DNS 服务器上，新建 xpc.cn、xpc.com、xpc.net 三个区域，并分别添加主机。

2．建立主目录

在 D 盘下，建立一个名称为 xpcncn 的文件夹，以作为网站 www.xpc.cn 的主目录；建立一个名称为 xpcncom 的文件夹，以作为网站 www.xpc.com 的主目录；建立一个名称为 xpcnnet 的文件夹，以作为网站 www.xpc.net 的主目录。

3．建立新网站www.xpc.net

在完成上述步骤后，接下来添加 www.xpc.net 网站。

（1）选择“开始→管理工具→Internet 信息服务（IIS）管理器”命令，打开“Internet 信息服务（IIS）管理器”窗口，右击“Internet 信息服务”树下“网站”选项，在弹出的菜单中选择“新建→网站”选项，弹出“网站创建向导”对话框，

（2）单击“下一步”按钮，弹出“网站描述”对话框，在“描述”栏中输入“第 2 个网站”。单击“下一步”按钮，弹出“IP 地址和端口设置”对话框，在“网站 IP 地址”下拉列表框中选择 IP 地址为“192.168.11.250”，在“网站 TCP 端口”栏中输入 8080，如图 9.69 所示。

（3）单击“下一步”按钮，弹出“网站主目录”对话框，在“路径”框中输入“D:\xpcnnet”或通过单击“浏览”按钮选择。

（4）单击“下一步”按钮，弹出“网站访问权限”对话框，默认选择即可。

（5）单击“下一步”按钮，完成设置。

4．修改TCP端口

如果要修改网站的 IP 地址，可以右击网站，选择“属性”选项，在“TCP 端口”框中更改 TCP 端口号。如图 9.70 所示。

5．建立新网站www.xpc.com和www.xpc.cn

按照建立新网站 www.xpc.net 的方法建立新网站 www.xpc.com 和 www.xpc.cn，注意将其 TCP 端口号分别改为 8090 和 80。主目录分别设为 D:\xpcncom 和 D:\xpcncn。

图 9.69　网站 TCP 端口

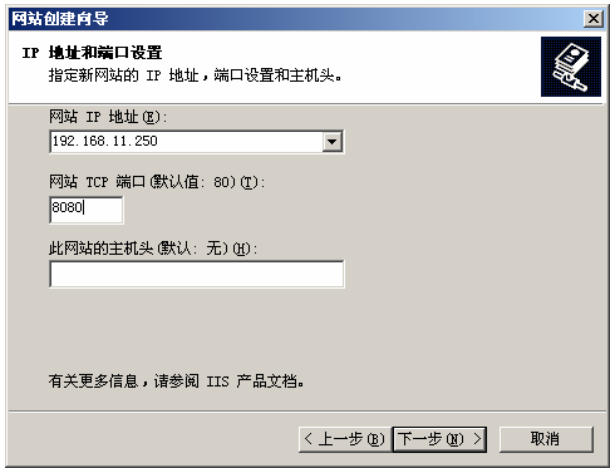

图 9.70　修改 TCP 端口号

6．利用浏览器来连接新网站

用户在浏览器内利用 http://www.xpc.com、http://www.xpc.net 和 http://www.xpc.cn 来连接网站。

习　题

一、名词解释

1．统一资源定位符

2．超文本传输协议

3．虚拟目录

二、填空题

1．_____是 Internet Information Server 的缩写，它是微软公司主推的信息服务器。

2．每个 Web 站点都具有唯一的、由 3 部分组成的标识用来接收和响应请求，它们分别是_____、_____和_____。

3．默认的 Web 站点的默认主目录是_____。

4．WWW 服务采用_____模式，客户机即_____，服务器即_____，它以_____和_____为基础，为用户提供界面一致的信息浏览系统。

5．用户使用浏览器总是从访问某个_____开始的。

6．HTTP 的 URL 的一般形式为_____，使用 FTP 访问站点的 URL 的形式为_____。

7．HTTP 会话过程包括_____、_____、_____、_____4 个步骤。

8．用户浏览页面的方法有_____、_____2 种。

9．IIS 6.0 默认的主页文档文件名可以为_____、_____、_____、_____等几种。

10．每一个 Web 站点都由_____、_____、_____3 部分组成识别数据，用以接收与回应客户端的要求，变更以上三者中任何一个，都可以在同一台计算机上架设多个站点。

三、选择题

1．浏览器与 Web 服务器之间使用的协议是（　　）。

A．DNS　　B．SNMP

C．HTTP　　D．SMTP

2．下列（　　）不是 IIS6.0 提供的组件。

A．Web　　B．FTP

C．TCP/IP　　D．SMTP

3．在 Internet 服务管理器中，可操作的对象不包括（　　）。

A．Web 或 FTP　　B．计算机

C．Web 或 FTP 目录　　D．DNS

4．Web 站点组成中，下列（　　）不是必须的识别数据。

A．端口编号　　B．IP 地址

C．主目录　　D．主机标题名称

5．默认 Web 服务器端口号是（　　）。

A．80　　B．81

C．21　　D．20

6．关于因特网中的 Web 服务，以下说法正确的是（　　）。

A．Web 服务器中存储的通常是符合 HTML 规范的文档

B．Web 服务器必须具有创建和编辑 Web 页面的功能

C．Web 客户端程序也称为 Web 浏览器

D．Web 服务器也称为 WWW 服务器

7．通过（　　）服务器，用户可以有效直观地将企业信息发布给企业内部用户和 Internet 远程用户。

A．FTP　　B．DHCP

C．DNS　　D．Web

8．一个 Web 站点，主机头是 www.abc.com，端口是 8080，则客户端访问该站点时，在 IE 浏览器的地址栏中的完整输入应该是（　　）。

A．http://www.abc.com　　B．http://www.abc.com/index.htm

C．http://www.abc.com/8080　　D．http://www.abc.com:8080

四、思考题

1．虚拟目录与普通目录有什么区别？

2．在 IIS6.0 中创建新站点的方法有几种？它们各自如何操作？

3．客户登录 Web 站点的方法有几种？

4．用户浏览 Web 服务的过程有哪几步？

五、实训题

在 Windows Server 2003 系统下利用 Apache 配置 Web 站点。

项目 10　架设单位内部FTP服务器

在 Internet 和 Intranet 中，FTP 是除 Web 之外最为广泛的一种应用，大量的软件及声音、视频等大容量文件的上传和下载多使用 FTP 方式。

10.1　项目内容

1．项目目的

在了解 FTP 工作原理和 IIS 操作特点的基础上，以 Windows Server 2003 操作系统为服务平台，掌握在 IIS 中创建和管理 FTP 站点的具体方法，并熟悉 FTP 客户端的使用方法。

2．项目任务

有一所高等院校，组建了学校的校园网，开发了学院网站，为了便于管理，需要将学院的 Web 服务器配置成 FTP 服务器，便于文件的上传和下载。

3．任务目标

① 熟悉 FTP 的工作原理；
② 了解 FTP 的应用特点；
③ 掌握 IIS 中 FTP 服务器的安装和配置方法；
④ 掌握 FTP 客户端的使用方法。

10.2　相关知识

FTP 至今未被 HTTP 完全取代的原因就是它的管理简单，且具备双向传输功能。在建立 FTP 站点之前，先了解 FTP 的基本知识是很有必要的。

10.2.1　什么是FTP

FTP（File Transfer Protocol）就是文件传输控制协议，是用于 TCP/IP 网络及 Internet 的最简单、广泛的协议之一。FTP 的主要作用是让用户连接上一个远程计算机（这些计算机运行着 FTP 服务进程，并且存储着各种格式的文件，包括计算机软件、声音文件、图像文件、重要资料、电影等），查看远程计算机上有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机去。前者称为“下载”，后者称为“上传”。

FTP 的一项突出优点就是可在不同类型的计算机之间传送文件。如 PC 机、服务器、小型机、大型机，以及 Windows 平台、Linux 平台、UNIX 平台，只要双方都支持 FTP，支持 TCP/IP 协议，就可以方便地交换文件。

FTP 是一个通过 Internet 传送文件的系统。Internet 上很多站点都提供了匿名 FTP 服务，允许任何用户访问该站点，并可从该站点免费复制文件。许多商业软件都是通过 FTP 发行的，不过下载时需要特定的账户。

FTP 服务要求用户登录服务器来使用服务。登录后，用户可指向 FTP 服务可用的目录。目前，FTP 服务主要用于以下 3 个方面：

- 提供软件下载的高速站点；
- Web 站点维护和更新；
- 在不同类型计算机之间传输文件。

10.2.2 FTP的工作原理

FTP 使用客户/服务器模式，即由一台计算机作为 FTP 服务器提供文件传输服务，而由另一台计算机作为 FTP 客户端提出文件服务请求并得到授权的服务。客户端和服务器端使用 TCP 进行连接，在连接时，都必须各自打开一个 TCP 端口。FTP 服务器预置两个端口：21 和 20。其中端口 21 用来发送和接收 FTP 的控制信息，一旦建立 FTP 会话，端口 21 的连接在整个会话期间始终保持打开状态；端口 20 用于发送和接收 FTP 数据，只有在传输数据时才打开，一旦传输结束就断开。FTP 客户端激发 FTP 客户端服务之后，动态分配自己的端口（端口号为 1024～65535）。

FTP 工作的过程就是一个建立 FTP 会话并传输文件的过程，如图 10.1 所示。具体传输过程如下：

① FTP 客户端程序向远程的 FTP 服务器申请建立连接；

② FTP 服务器的端口 21 侦听到 FTP 客户端的请求之后，做出响应，与其建立会话连接；

③ 客户端程序打开一个控制端口，连接到 FTP 服务器的端口 21；

④ 需要传输数据时，客户端打开一个数据端口（使用 netstat），连接到 FTP 服务器的端口 20，文件传输完毕后断开连接，释放端口；

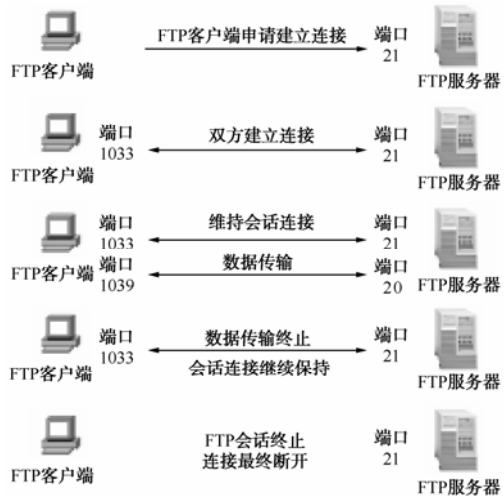

图 10.1 FTP 工作过程

⑤ 要传输新的文件时，客户端会再打开一个新的数据端口，连接到 FTP 的端口 20；

⑥ 空闲时间超过规定后，FTP 会话自行终止，也可由客户端或服务器端强行断开连接。

10.2.3 匿名FTP和用户FTP

用户对 FTP 服务的访问有两种方式：匿名 FTP 和用户 FTP。

1．匿名FTP

所谓匿名就是允许任何用户访问 FTP 服务器并下载文件，无论用户是否拥有该 FTP 服务器的账户，都可以使用“anonymous”用户名进行登录，一般以自己的 E-mail 地址作为密码。

2．用户 FTP

这种方式为已在 FTP 服务器上建立特定账户的用户使用，必须以用户名和口令来登录。但当用户从 Internet 与 FTP 服务器连接时，所使用的口令以明文形式传输，接触系统的任何人都可以使用相应的程序获取该用户的账户和口令。

在一般情况下，在许多 FTP 站点上，都可以自动匿名登录，从而查看或下载文件。要上载、重命名或删除文件，可能需要特殊的用户名和密码登录。同时，相同站点的不同区域也可能需要进行不同的登录。

10.2.4 主动模式和被动模式

根据 FTP 数据连接建立方法，可将 FTP 客户端对 FTP 服务器端的访问分为两种模式：主动模式（又称标准模式）和被动模式。

1．主动模式FTP

主动模式的 FTP 是这样的：客户端从一个任意的非特权端口 N（N>1024）连接到 FTP 服务器的命令端口，也就是端口 21。然后客户端开始监听端口 N+1，并发送 FTP 命令“port N+1”到 FTP 服务器。接着服务器会从它自己的数据端口（20）连接到客户端指定的数据端口（N+1）。

主动模式 FTP 的主要问题实际上在于客户端。FTP 的客户端并没有实际建立一个到服务器数据端口的连接，它只是简单的告诉服务器自己监听的端口号，服务器再回来连接客户端这个指定的端口。

2．被动模式FTP

为了解决服务器发起到客户的连接的问题，人们开发了一种不同的 FTP 连接方式。这就是被动模式，或者叫做 PASV，当客户端通知服务器它处于被动模式时才启用。

在被动模式 FTP 中，命令连接和数据连接都由客户端，这样就可以解决从服务器到客户端的数据端口的入方向连接被防火墙过滤掉的问题。当开启一个 FTP 连接时，客户端打开两个任意的非特权本地端口（N > 1024 和 N+1）。第一个端口连接服务器的端口 21，但与主动模式 FTP 不同，客户端不会提交 port 命令并允许服务器来回连接它的数据端口，而是提交 PASV 命令。这样做的结果是，服务器会开启一个任意的非特权端口（P > 1024），并发送 port P 命令给客户端。然后客户端发起从本地端口 N+1 到服务器的端口 P 的连接用来传送数据。

主动模式 FTP：

命令连接：客户端＞端口 1024－＞服务器端口 21

数据连接：客户端＞端口 1024＜－服务器端口 20

被动模式 FTP：

命令连接：客户端＞端口 1024－＞服务器端口 21

数据连接：客户端＞端口 1024－＞服务器端口>1024

下面是主动模式与被动模式优缺点的简要总结：

主动模式 FTP 对 FTP 服务器的管理有利，但对客户端的管理不利。因为 FTP 服务器企图与客户端的高位随机端口建立连接，而这个端口很有可能被客户端的防火墙阻塞掉。被动模式 FTP 对 FTP 客户端的管理有利，但对服务器端的管理不利。因为客户端要与服务器端建

立两个连接，其中一个连到一个高位随机端口，而这个端口很有可能被服务器端的防火墙阻塞掉。

10.2.5 FTP命令

用户可以使用 FTP 命令来进行文件传输，称为交互模式。当用户交互使用 FTP 时，FTP 发出一个提示，用户输入一条命令，FTP 执行该命令并发出下一提示。FTP 允许文件沿任意方向传输，即文件可以上传与下载，在交互方式下，也提供了相应的文件上传与下载的命令。如在 Windows Server 2003 操作系统下可使用如下形式的 FTP 命令。

FTP [-d-g-i-n-t-v] [host]

其中：

- host：代表主机名或者主机对应的 IP 地址。
- -d：表示允许调试。
- -g：表示不允许在文件名中出现“*”和“?”等通配符。
- -i：表示多文件传输时，不显示交互信息。
- -n：表示不利用$HOME/netrc 文件进行自动登录。
- -t：表示允许分组跟踪。
- -v：显示所有从远程服务器上返回的信息。
- []：表示其中的内容为命令的可选参数。

用户输入 FTP 命令如“ftp://192.168.11.250”后，屏幕就会显示“FTP >”提示符，表示用户进入 FTP 交互模式，在该模式下用户可输入 FTP 操作的子命令。常见的 FTP 子命令及其功能如下：

- ASCII：进入 ASCII 方式，传送文本文件；
- BINARY：传送二进制文件，进入二进制方式；
- BYE 或 QUIT：结束本次文件传输，退出 FTP 程序；
- CD dir：改变当前工作目录；
- LCD dir：改变本地当前目录；
- DIR 或 LS [remote-dir] [local-file]：列目录；
- GET remote-file [local-file]：获取远地文件；
- MGET remote-files：获取多个远地文件，可使用通配符；
- PUT local-file [remote-file]：将一个本地文件传递到远地主机上；
- MPUT local-files：将多个本地文件传到远地主机上，可用通配符；
- DELETE remote-file：删除远地文件；
- MDELETE remote-files：删除多个远地文件；
- MKDIR dir-name：在远地主机上创建目录；
- RMDIR dir-name：删除远地目录；
- OPEN host：与指定主机的 FTP 服务器建立连接；
- CLOSE：关闭与远地 FTP 程序的连接；
- PWD：查询当前目录；
- STATUS：显示 FTP 程序的状态；
- USER user-name [password] [account]：向 FTP 服务器表示用户身份。

还有许多工具软件被开发出来用于实现 FTP 的客户端功能，如 NetAnts、Cute FTP、WSFTP 等，另外 Internet Explorer 和 Netscape Navigator 也提供 FTP 客户软件的功能。这些软件的共同特点是采用直观的图形界面，通常还实现了文件传输过程中的断点再续和多路传输功能。

10.2.6 FTP文件传输类型

FTP 有文本方式与二进制方式两种文件传输类型，所以用户在进行文件传输之前，还要选择相应的传输类型：根据远程计算机文本文件所使用的字符集是 ASCII 或 EBCDIC，用户可以用 ASCII 或 EBCDIC 命令来指定文本方式传输；二进制文件是指非文本文件如压缩文件、图形与图像、声音文件、电子表格、计算机程序、电影或其他文件，都必须用二进制方式传输，用户输入 binary 命令可将 FTP 转换成二进制模式。

10.2.7 FTP服务器软件

许多综合性的 Web 服务器软件，如 IIS、Apache 等，都集成了 FTP 功能。目前有许多 FTP 服务器软件可供选择，这些软件都比较小，并且共享和免费的居多。Serv-U 是一种使用广泛的 FTP 服务器软件。

10.2.8 简单文件传输协议TFTP

TFTP 是一个很小且易于实现的文件传输协议。TFTP 也采用客户/服务器模式，使用 UDP 数据报。TFTP 没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份认证。

TFTP 可用于 UDP 环境，而且 TFTP 代码所占的内存较小。每次传送的数据有 512 字节，但最后一次可不足 512 字节；可支持 ASCII 码或二进制传送；可对文件进行读或写。

在开始工作时，TFTP 客户进程发送一个读请求 PDU 或写请求 PDU 给 TFTP 服务器进程，其端口号为 69。TFTP 服务器进程要选择一个新的端口和 TFTP 客户进程进行通信。TFTP 共有 5 种协议数据单元 PDU，即读请求 PDU、写请求 PDU、数据 PDU、确认 PDU 和差错 PDU。

TFTP 协议被 Cisco 的网络设备用来作为操作系统和配置文件的备份工具。在 Cisco 网络设备组成的网络里，可以用一台主机或服务器作为 TFTP 服务器，并且把网络中各台 Cisco 设备的 IOS 和配置文件备份到这台 TFTP 服务器上，以防备可能的严重故障或人为因素使网络设备的 IOS 或运行配置丢失。当发生这种情况时，可以方便快速地通过 TFTP 协议从 TFTP 服务器上把相应的文件传送到网络设备中，及时恢复设备以正常工作。

10.3 方案设计及准备

1．设计

架设一台基于 Windows Server 2003 系统下 IIS 的 FTP 服务器，要求如下：

- 服务器端：在一台安装 Windows Server 2003 系统的计算机（IP 地址为 192.168.11.250，子网掩码为 255.255.255.0，网关为 192.168.11.1）上设置 1 个 FTP 站点，端口为 21，FTP 站点标识为“FTP 站点训练”；连接限制为 100 000 个，连接超时 120s；日志采用 W3C 扩展日志文件格式，新日志时间间隔为每天；启用带宽限制，最大网络使用 1 024 KB/s；主目录为

D:\ftpserver 目录；虚拟目录为 D:\ftpxuni，允许用户浏览和下载。

➢ 客户端：在 IE 浏览器的地址栏中输入 ftp://192.168.11.250 来访问刚才创建的 FTP 站点。配合项目4　DNS 服务器的配置，将 IP 地址 192.168.11.250 与域名 ftp://ftp.xpc.edu.cn 对应起来，在 IE 浏览器的地址栏中输入 ftp://ftp.xpc.edu.cn 来访问刚才创建的 FTP 站点。

根据以上要求，本项目实施的网络拓扑图如图 10.2 所示。

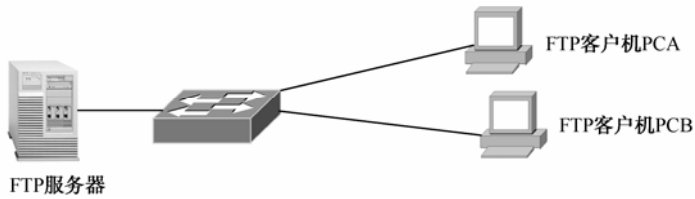

图 10.2　FTP 服务网络拓扑图

2．材料清单

为了搭建图 10.2 所示的网络环境，需要下列设备：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② Windows XP 计算机 2 台；

③ 以上两台计算机已联入因特网。

10.4　项目实施

步骤 1：硬件连接

按照图 10.2 所示，搭建 FTP 服务器配置网络模型图。

步骤 2：设置IP地址及测试连通性

设置各计算机的 IP 地址、子网掩码、网关，见表 10.1。

表 10.1　计算机网络设置

计算机	IP 地址	子网掩码	网关
FTP 服务器	192.168.11.250	255.255.255.0	192.168.11.1
PCA	192.168.11.10	255.255.255.0	192.168.11.1
PCB	192.168.11.11	255.255.255.0	192.168.11.1

使用 ping 测试各计算机之间的连通性。除非全通继续进行，否则检测网线及计算机的配置，直到各计算机之间全部连通。

步骤 3：安装 Internet 信息服务和 FTP 服务

由于 FTP 依赖 Microsoft 网络信息服务（IIS），因此计算机上必须安装 IIS 和 FTP 服务。在一台安装了 IIS 6.0 的服务器中可以安装多个 FTP 站点主机，而不需要为每个 FTP 站点设置一个专用的服务器。

注意：在 Windows Server 2003 系统中，安装 IIS 时不会默认安装 FTP 服务。如果已在计算机上安装了 IIS，必须使用“控制面板”中的“添加或删除程序”工具安装 FTP 服务。

（1）选择“开始→控制面板→添加或删除程序→添加/删除 Windows 组件”命令。

（2）在“组件”列表中，选中“应用程序服务器”选项，选中“Internet 信息服务（IIS）”选项，然后单击“详细信息”按钮，打开“应用程序服务器子组件”窗口。

（3）选中“公用文件”、“文件传输协议（FTP）服务”、“Internet 信息服务管理器”复选框（如果它们尚未被选中）。

（4）选中想要安装的任何其他的 IIS 相关服务或子组件旁边的复选框，然后单击“确定”按钮。

（5）单击“下一步”按钮。出现提示时，将 Windows Server 2003 CD-ROM 插入计算机的 CD-ROM 或 DVD-ROM 驱动器，或提供文件所在位置的路径，然后单击“确定”按钮。单击“完成”按钮。

IIS 和 FTP 服务现已安装。下面再配置 FTP 服务，然后才能使用它。

步骤 4：新建FTP站点

默认 FTP 站点的主目录是\inetpub\ftproot，所以只需将欲实现共享的文件复制到\inetpub\ftproot 文件夹中，用户即可通过 ftp 客户端以匿名方式登录到该 FTP 服务器，实现文件的下载。但由于默认状态下主目录为只读方式，因此用户只能下载而无法上传。

如果用户希望添加新的 FTP 站点，可以执行以下步骤：

（1）右击“Internet 信息服务”树下的“FTP 站点”，在弹出的快捷菜单中选择“新建→FTP 站点”选项，弹出“FTP 站点创建向导”对话框，按照向导完成新建 FTP 站点。

（2）单击“下一步”按钮，弹出“FTP 站点描述”对话框，如图 10.3 所示。在“描述”文本框中输入 FTP 站点的描述，如输入“FTP 站点训练”。

（3）单击“下一步”按钮，弹出“IP 地址和端口设置”对话框，如图 10.4 所示。在“输入此 FTP 站点使用的 IP 地址”文本框中输入 FTP 站点的 IP 地址，如输入“192.168.11.250”。

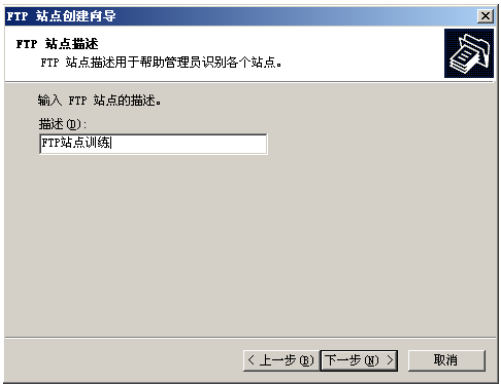

图 10.3 “FTP 站点描述”对话框

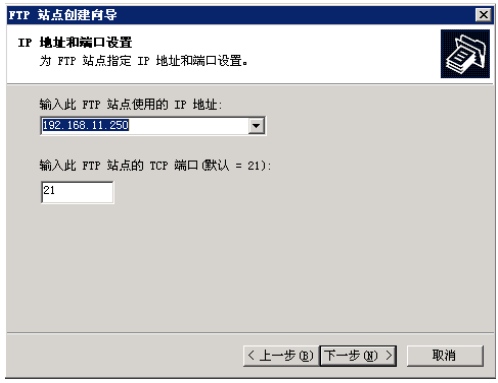

图 10.4 “IP 地址和端口设置”对话框

（4）单击“下一步”按钮，弹出“FTP 用户隔离”对话框，如图 10.5 所示。选中“不隔离用户”选项。

（5）单击“下一步”按钮，弹出“FTP 站点主目录”对话框，如图 10.6 所示。 在“路径”文本框中输入“D:\ftpserver”。单击“下一步”按钮，弹出“FTP 站点访问权限”对话框，选取权限，如选中“读取”复选框。单击“下一步”按钮，单击“完成”按钮，完成 FTP 站点的创建。

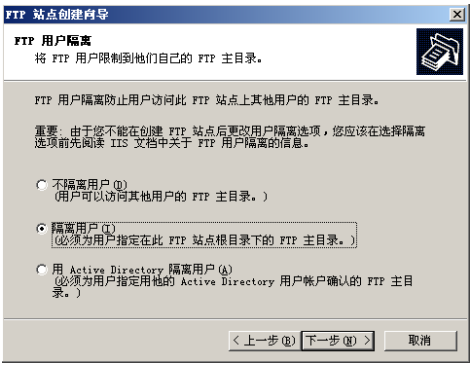

图 10.5　“FTP 用户隔离”对话框

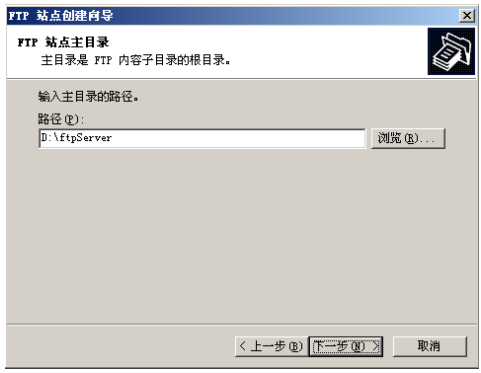

图 10.6　“FTP 站点主目录”对话框

步骤 5：FTP站点的配置

为了使 FTP 站点能够正常工作，还必须对 FTP 站点进行合理配置。

FTP 站点配置都是在要配置的 FTP 站点属性对话框中进行的。首先选择要配置的 FTP 站点，如“FTP 站点训练”，用鼠标右击该 FTP 站点选择“属性”选项，弹出“FTP 站点训练属性”对话框，如图 10.7 所示，由 5 个选项卡组成，可以分别对 FTP 站点各个方面的属性进行配置。

1）设置 FTP 站点标识

在图 10.7 所示的“FTP 站点训练属性”对话框中。对 FTP 站点属性配置的方法如下：

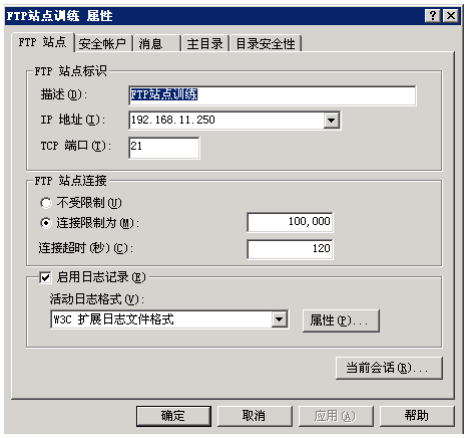

图 10.7　FTP 站点训练属性

（1）在“FTP 站点标识”区域，可以修改站点描述、FTP 站点使用 IP 地址、TCP 端口等信息。这些信息都是在创建 FTP 站点时指定的。

（2）在“描述”栏中可以设置该 FTP 站点的标识。该标识对于用户的访问没有任何意义，其作用只是当服务器中安装多个 FTP 服务器时，便于网络管理员进行区分，即站点标识将作为 FTP 服务器的名称显示在“Internet 信息服务”窗口目录树中。

（3）在“IP 地址”下拉列表中可以为该站选择一个 IP 地址，该 IP 地址必须是在“网络连接→本地连接”中配置给当前计算机（网卡）的 IP 地址。由于 Windows Server 2003 可安装多块网卡，并且每块网卡可绑定多个 IP 地址，因此，服务器可以拥有多个 IP 地址。如果这里不分配 IP 地址，即选用“全部未分配”，该站点将响应所有未分配给其他站点的 IP 地址，即以该计算机默认站点的身份出现。当用户向该计算机的一个 IP 地址发出连接请求时，如果该 IP 地址没有被分配给其他站点使用，将自动打开这个默认站点。

（4）在“TCP 端口”文本框中为站点指定一个 TCP 端口以运行服务，默认的 TCP 端口号是 21。也可以设置其他任意一个唯一的 TCP 端口，这时在客户端需以“IP：TCP Port”的格式访问，否则将无法连接到该站点。

（5）在“FTP 站点连接”区域中，可以设置站点的连接属性，这些属性通常决定了站点的访问性能。例如，默认的连接超时为 120s，如果一个连接与 FTP 站点未交换信息的时间达到指定的连接超时时间，FTP 站点将中断该连接。

（6）日志是以文件形式监视网站使用情况的手段。选中“启用日志记录”复选框，然后在“活动日志格式”下拉列表框中指定日志格式，各种日志格式的内在差别并不是很大，常用的日志格式有以下 3 种：

- “Microsoft IIS 日志文件格式”是一种固定的 ASCII 格式；
- “W3C 扩展日志文件格式”是一种可以自行定制的格式；
- “ODBC 日志”将记录保存到数据库。

选用一种格式（默认格式是 W3C 扩展日志文件格式）后，单击“属性”按钮可以对日志进行设置。

选定日志文件类型后，单击“属性”按钮，打开如图 10.8 所示的“日志记录属性”对话框。“常规”标签提供了一般性的日志文件设置界面。可以在“日志文件目录”栏中更改日志文件存储的路径。日志是一种持续性的记录手段，随着时间的推移，单个日志文件所记录的事件越来越多，也越来越大。为了防止日志文件太大所导致的存储及分析困难，应该在日志文件达到一定大小的时候新建一个文件。通常的判断方法有两种：一定时间后新建文件和达到一定大小后新建文件。对于前者，只需选择“每小时”、“每天”、“每周”或“每月”，即可在指定时间到达时自动生成新的日志文件，新文件将以时间命名，如 yymmdd.log 或 mmdd.log。而选择“当文件大小达到”并指定大小后，系统就可以在日志文件达到指定大小后生成新文件，默认情况下，每达到 20 MB 就要生成一个新文件。

在图 10.8 中单击“高级”标签，弹出“日志记录属性高级”对话框，如图 10.9 所示。可以指定日志文件记录何种事件及相关对象的细节。只需选取相应对象前面的复选框即可。例如，如果需要记录客户访问站点内容所使用的服务器端口号，就选择“服务器端口”前面的复选框。

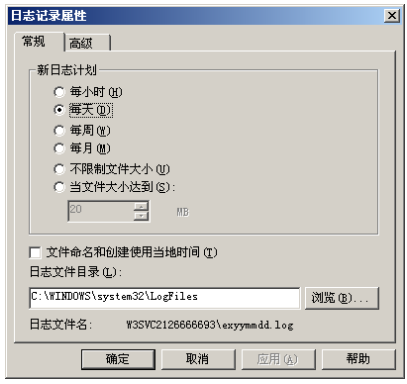

图 10.8　日志记录属性-常规

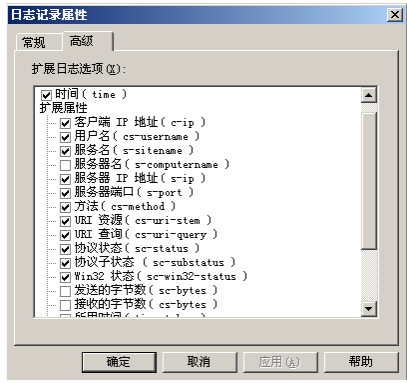

图 10.9　日志记录属性-高级

2）设置匿名账户

匿名账户的设置，可在“安全账号”选项卡中完成，如图 10.10 所示。

（1）允许匿名连接：选中“允许匿名连接”复选框，任何用户都可以使用“匿名（anonymous）”作为用户名登录到 FTP 服务器上。允许匿名连接后，对资源的所有请求都不会提示用户输入用户名或密码，而是默认由 IIS 自动创建的名为 IUSR_ computername（其中 computername 为 FTP 服务

器的计算机名，本机为 xxzx-chujl）的 Windows 用户账户，作为其用户名。

如果不选该复选框，用户在登录到 FTP 服务器时，需要输入有效的 Windows 用户名和密码。如果 FTP 服务器不能证实用户的身份，服务器将返回错误消息。

图 10.10“安全账号”对话框

（2）用户名：该用户名为在匿名连接时使用的用户名，默认为 IUSR_computername。若欲另行选用其他的 Windows 用户账户，可单击“浏览”按钮，在弹出的“选择用户”对话框中选择。为了 FTP 服务器数据的安全，还是采用默认的、拥有最低权限的 IUSR_ computername 作为匿名账户。

（3）密码：在图 10.10 所示对话框中的“密码”栏中输入匿名连接账户使用的密码。如果选中了“允许 IIS 控制密码”选项，密码将不能更改。

（4）只允许匿名连接：选中“只允许匿名连接”复选框之后，用户就不能使用用户名和密码登录。选用该复选框可避免具有管理权限的账户访问，而仅允许指定为匿名的账户访问。由于匿名用户往往是权限最低的用户，因此，在特殊情况下有助于保护数据安全。

3）FTP 站点消息

FTP 站点消息是在“FTP 站点训练属性”对话框中的“消息”选项卡中进行指定的。FTP 站点消息分为 4 种：标题、欢迎、退出、最大连接数，分别在“消息”选项卡中的“标题”、“欢迎”、“退出”和“最大连接数”栏中进行指定。如图 10.11 所示。

4）配置 FTP 站点主目录

FTP 站点主目录是指映射为 FTP 根目录的文件夹，FTP 站点中的所有文件全部保存在该文件夹中，而且当用户访问 FTP 站点时，也只有该文件夹中的内容可见，并且作为该 FTP 站点的根目录。

（1）修改主目录位置。FTP 站点主目录的位置可以指定本地计算机中的其他文件夹，甚至是另一台计算机上的共享文件夹。

① 此计算机上的目录。如图 10.12 所示，本地主目录的指定方法为：在“主目录”选项卡中选择主目录位置为“此计算机上的目录”。单击“浏览”按钮，指定主目录位置或者直接在“本地路径”栏中输入主目录路径。单击“应用”按钮、“确定”按钮完成。

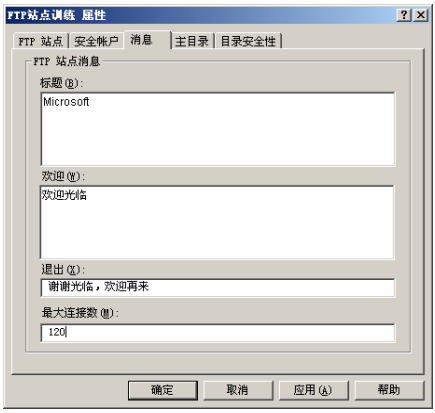

图 10.11 “消息”对话框

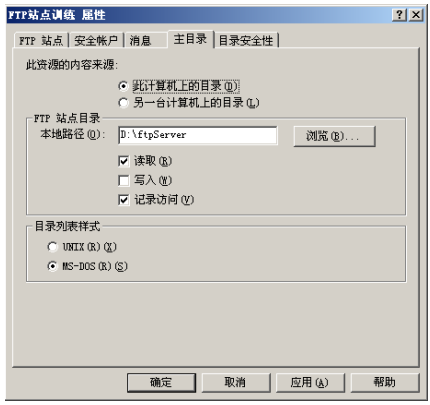

图 10.12 “主目录”对话框

② 另一台计算机上的共享位置。在“主目录”选项卡中选择主目录位置为“另一计算机上的共享位置”，然后从“网络共享”栏中指定共享主目录的 UNC 路径。

（2）修改访问权限。

- 读取：选择“读取”选项，允许用户阅读或下载存储在主目录或虚拟目录中的文件。
- 写入：选择“写入”选项，允许用户向服务器中已启用的目录上传文件。仅对那些可能接受用户文件的目录选择该选项。

（3）目录列表风格。在“主目录”选项卡中还可以指定目录列表风格。可选的站点目录列表风格有 MS-DOS 和 UNIX 两种，在“主目录”选项卡中的“目录列表风格”栏中选择“MS-DOS”或“UNIX”。这两种风格分别适用于 DOS/Windows 用户和 UNIX 用户。

步骤 6：IIS的FTP安全管理

IIS 的 FTP 安全管理也是以 Windows 操作系统和 NTFS 文件系统的安全性为基础的。FTP 的安全问题主要是解决访问控制问题，即让特定的用户能够访问特定的资源，既要控制 FTP 用户及其使用的计算机或网络，又要确定特定的资源（站点、目录和文件）可让特定的用户访问。当用户访问 FTP 服务器时，IIS 利用其本身和 Widnows 操作系统的多层安全检查和控制来实现有效的访问控制。具体的访问控制包括：

① FTP 服务器检查 FTP 服务客户使用的 IP 地址；

② 检查 FTP 用户是否拥有有效的 Windows 用户账户；

③ IIS 检查用户是否具有请求资源的访问权限；

④ IIS 检查资源的 NTFS 权限。

这些设置与 Web 安全管理类似，在这里不再详述。

步骤 7：FTP站点的启动与停止

如果 FTP 站点当前为“停止”状态，那么可以通过单击“活动工具栏”中的“启动项目”按钮或右击该站点，从弹出的快捷菜单中执行“启动”选项，来启动该 FTP 站点。如果 FTP 站点当前为“启动”状态，那么可以通过单击“活动工具栏的”中的“停止项目”按钮或右击该站点，从弹出的快捷菜单中执行“停止”选项，来停止该 FTP 站点。

步骤 8：创建虚拟目录

用户可以在 FTP 站点中创建虚拟目录。虚拟目录是指在物理上并非包含在 FTP 站点主目录中的目录，但对于访问 FTP 站点的用户来说，该目录又好像确实存在。实际上，创建虚拟目录就是建立一个到实际目录的指针，实际目录下的内容并不需要迁移到 FTP 站点的主目录下。创建虚拟目录的过程如下。

（1）选择要在其中创建虚拟目录的 FTP 站点，如 FTP 站点训练，鼠标右击该站点，在弹出的菜单中选择“新建→虚拟目录”选项，弹出“虚拟目录创建向导”对话框。

（2）用户按照“虚拟目录创建向导”的要求，分别在“别名”框中输入“ftpxuni”、“路径”框中输入“D:\ftpxuni”、“权限”列表中选择“读取”等信息。一旦输入完成，系统将在“FTP 站点训练”站点下创建一个虚拟目录。

（3）虚拟目录浏览，打开 IE 浏览器，在“地址栏”中输入“ftp://IP 地址/目录名”或“ftp://域名/目录名”，如 ftp://192.168.11.250/ ftpxuni 或 ftp://www.xpc.edu.cn/ ftpxuni，即可直接浏览建立的虚拟目录。

步骤 9：利用Web浏览器访问FTP站点

Web 浏览器除了可以访问 Web 站点以外，还可以访问 FTP 站点，浏览 FTP 站点中的文件夹和文件，并实现文件的下载。在访问 FTP 站点时，在浏览器地址栏中输入的内容稍有不同。

1）访问 FTP 站点

运行 Web 浏览器，如 Internet Explorer，并在地址栏中输入欲连接的 FTP 站点的 Internet 地址或域名，如 ftp://192.168.11.250 或 ftp://ftp.xpc.edu.cn。此时，将在浏览器中显示该 FTP 站点主目录中所有的文件夹和文件，如图 10.13 所示。

如果 FTP 站点采用 Windows 身份验证，而要求用户输入用户名和密码，则需要在地址中包括这些信息，格式为“ftp://用户名:密码@ftpIPaddress”。

（1）浏览和下载。当该 FTP 站点只被授予“读取”权限时，则只能浏览和下载该站点中的文件夹和文件。

➢ 浏览的方式非常简单，只需用鼠标双击即可打开相应的文件夹和文件。

➢ 若欲下载，只需单击鼠标右键，并在弹出的快捷菜单中选择“复制”，而后打开 Windows 资源管理器，将该文件或文件夹粘贴到欲保存的位置即可，如图 10.14 所示。

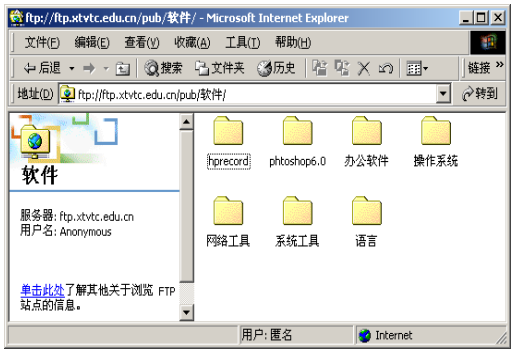

图 10.13　ftp://ftp.xpc.edu.cn 站点

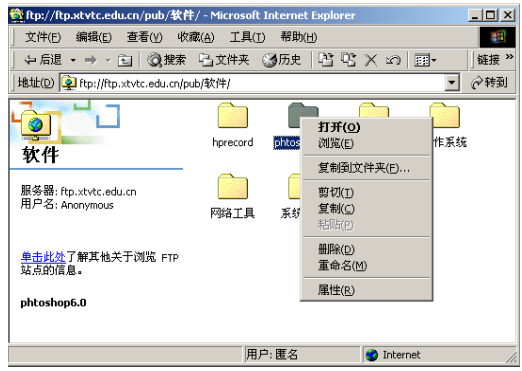

图 10. 14　下载文件

（2）重命名、删除、新建文件夹和文件上传。当该 FTP 站点被授予“读取”和“写入”权限时，则不仅能够浏览和下载该站点中的文件夹和文件，而且还可以直接在 Web 浏览器中实现新文件的建立，以及对文件夹和文件的重命名、删除和文件的上传。

➢ 在 Web 浏览器中重命名和删除 FTP 站点中文件夹和文件的方式，与在 Windows 资源管理器中相同。

➢ 在目标文件夹的空白处单击鼠标右键，并在弹出的快捷菜单中选择“新建文件夹”，即可在当前文件夹下建立一个新文件夹。

➢ 通过 Web 浏览器向 FTP 站点上传文件夹和文件，先打开 Windows 资源管理器，选中并复制欲上传的文件夹和文件，然后在 Web 浏览器中浏览并找到目标文件夹，而后在浏览器的空白处单击鼠标右键，在弹出的快捷菜单中选择“粘贴”即可。

2）访问虚拟目录

打开 Web 浏览器，在“地址栏”中输入“ftp://IP 地址/目录名”或“ftp://域名/目录名”，即可浏览虚拟目录中的所有文件。

当需要使用用户名和密码访问时，采用的格式为“ftp://用户名:密码@IP 地址/目录名”或“ftp://用户名:密码@域名/目录名”。

通过 Web 浏览器对虚拟目录中文件的操作与在 FTP 站点中的操作完全相同，可根据虚拟目录的访问权限不同，分别进行浏览、重命名、删除、下载、上传和文件夹的建立。

步骤 10：利用FTP客户端访问FTP站点

FTP 服务借助于 FTP 客户端有时比 Web 浏览器更方便，下面以 WSFTP 为例简要介绍一下如何实现对 FTP 站点的访问。

（1）运行 WSFTP。

（2）在“Connection”对话框右侧的文本框中依次输入相关信息，如 Host Name（FTP 站点 IP 地址或域名）、UserID（用户名，匿名登录时可以为空）、Password（密码，匿名登录时可以为空）等，如图 10.15 所示。

单击“Connect”按钮，尝试实现与 FTP 站点的连接。登录成功后的界面如图 10.16 所示。其中，左侧栏为本地硬盘中的文件夹列表，右侧栏为 FTP 站点中根目录下的文件列表。若上传文件，需要先调整 FTP 站点的当前文件夹，然后选中左侧栏中欲上传的文件，单击“ ”按钮，即可完成上传。若下载文件，需要先选中本地硬盘的当前文件夹，然后选中右侧栏中欲下载的文件，单击“ ”按钮，即可完成下载。

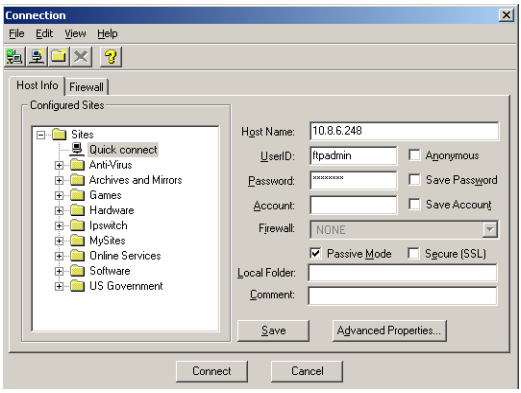

图 10.15 “Connection”对话框

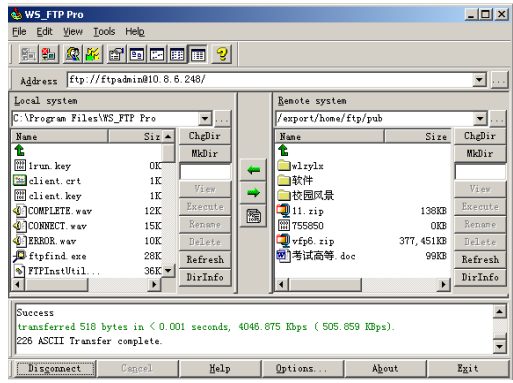

图 10.16 “WS_FTP PRO”登录成功界面

（3）操作完成后，单击工具栏中的“Disconnect”按钮，终止与 FTP 服务器的连接。

10.5 扩展知识及任务训练

10.5.1 训练 1：使用FTP用户隔离

“隔离用户”是 IIS 6.0 中包含的 FTP 组件的一项新增功能。配置成“用户隔离”模式的 FTP 站点可以使用户登录后直接进入属于该用户的目录中，而且该用户不能查看或修改其他用户的目录。

隔离模式只能在创建 FTP 站点时设置，设置之后不能更改。默认 FTP 站点使用的是“不隔离用户”。

在 IIS 6.0 中为用户 wangluo001 和 wangluo002 两个用户创建隔离的 FTP 服务。

1．创建不同的用户账号

执行“开始→程序→管理工具→计算机管理”，创建 wangluo001 和 wangluo002 两个用户。

2．规划文件夹结构，创建各用户对应的子文件夹

在 IIS 6.0 中启用隔离用户，所有的用户主目录都在 FTP 站点目录中的二级目录结构下。

首先必须在 NTFS 分区中创建一个文件夹作为 FTP 站点的主目录（如“我的 FTP”），然后在“我的 FTP”文件夹下创建一个名为“LocalUser”的子文件夹，最后在“LocalUser”文件夹下创建若干个跟用户账户一一对应的个人文件夹，如 wangluo001 和 wangluo002 两个文件夹。

另外，如果想允许用户使用匿名方式登录“用户隔离”模式的 FTP 站点，则必须在“LocalUser”文件夹下面创建一个名为“Public”的文件夹。

3．安装IIS 6.0，并设定FTP服务，选择“隔离用户”

（1）在 FTP 站点创建过程中，选择“隔离用户”选项。

（2）设置 FTP 站点属性。

用鼠标右击 FTP 站点，选择“属性”命令，选中“安全账户”选项卡，选中“允许匿名连接”复选框，在“用户名”和“密码”框中输入用于验证匿名用户的用户码和密码。

10.5.2 训练 2：利用Serv−U组建FTP站点

在 Windows Server 2003 集成的 IIS 中带有 FTP 组件，但 Microsoft 提供的这项服务并不完美，在这里以一个实例来介绍如何利用 Serv-U 来组建 FTP 站点。

在这里假设本机 IP 地址是 192.168.11.250，本机计算机名为 xxzx-chujl，在 D 盘建立了 ftpserver 文件夹，并在此文件夹下创建了 anon、Wlzx、Xxzx、pub 4 个文件夹，在 ftpserver 文件夹下创建 2 个文本文件，名称分别为“登录消息.txt”和“用户注销.txt”。允许匿名访问（Anonymous），匿名用户登录后进入的将是 D:\ftpserver\anon 目录；创建用户 chujl 和 liuyf，其中 chujl 的用户文件夹为 D: \ftpserver\wlzx，liuyf 的用户文件夹为 D: \ftpserver\xxzx。文件夹 pub 可以让所有的用户访问。

在所有的 FTP 服务器端软件中，Serv-U 除了拥有其他同类软件所具备的几乎全部功能外，还支持断点续传、支持带宽限制、支持远程管理、支持远程打印、支持虚拟主机等。

1．Serv-U的基本情况

软件名称：Serv-U FTP Server 6.1.0.5（共享软件）；

运行环境：除 Windows 3.x 之外的全系列版本；

下载地址： http://www.serv-u.com 及其他软件下载网站等。

2．安装

直接双击 susetup.exe 文件，开始安装工作。除了在出现使用协议那一步中，需要选中“I have checked my McAfee settings or don’t use it”和“I have read and accept the above license agreement”之外，其他均使用其默认选项即可。

当安装完成后，系统将自动进入 Serv-U Administrator（以下简称“管理器”）的窗口，开始 Serv-U 的初始配置，步骤如下：

（1）在 Setup Wizard（安装向导）对话框中，如图 10.17 所示。单击“Next”按钮，开始

FTP Server 的基本配置。弹出“Show Menu Images”对话框，单击“Yes”按钮。

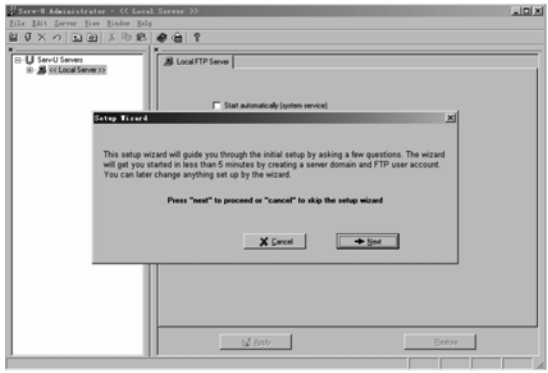

图 10.17　Serv-U 安装向导

（2）单击“Next”按钮，弹出“Start Local Server”对话框，单击“Next”按钮，弹出 Serv-U”的主界面，系统自动配置，弹出“Your IP address”对话框，如图 10.18 所示，在“IP address ,leave blank for dynamic or unknown IP”文本框中输入 FTP 服务器的 IP 地址，如 192.168.11.250。

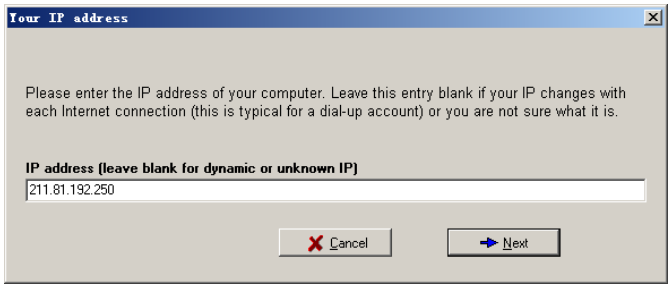

图 10.18　“Your IP address”对话框

（3）单击“Next”按钮，弹出“Domain Name”对话框，如图 10.19 所示。在“Domain Name”文本框中输入 FTP 服务器的域名，如 xpc.edu.cn。

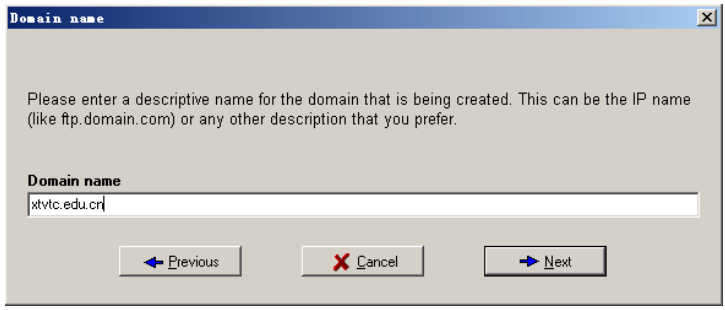

图 10.19　“Domain Name”对话框

（4）单击“Next”按钮，弹出“system service”对话框，选择是否把 Serv-U 安装成系统服务，以便让 Serv-U 提供 FTP 服务器与系统一同启动。推荐安装，单击“Yes” 按钮。

（5）单击“Next”按钮，弹出“anonymous account”对话框，单击“Yes” 按钮允许匿名访问。

（6）单击“Next”按钮，弹出“home directory”对话框，如图 10.20 所示，设定匿名用

户登录后其虚拟根目录在 FTP 服务器上的真实位置，如 D:\ftpserver\anon。

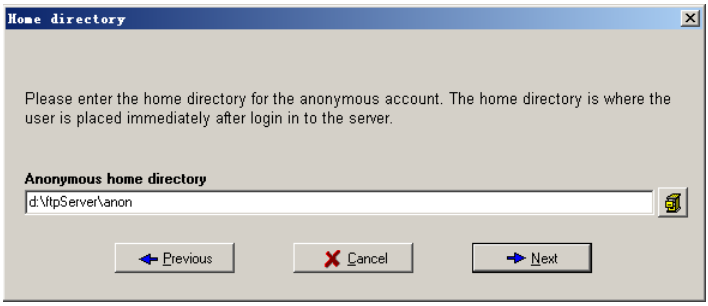

图 10.20　“Home Directory”对话框

（7）单击“Next”按钮，弹出“Lock in home directory”对话框，单击“Yes” 按钮，则匿名用户只能访问其主目录及以下的目录树；如果单击“No” 按钮，则它还可以访问其主目录的同级或更高级的目录树。从安全角度考虑，一般建议选“Yes”。此时就可以根据这个向导开始建立你的第一个 FTP 服务器。

（8）单击“Next”按钮，弹出“Name Account”对话框，询问是否直接建立普通用户（相对匿名用户而言）账号。单击“No” 按钮，单击“Next” 按钮，暂时停止创建用户。单击“Finish”按钮完成 FTP 安装。当安装完成后，即可以在管理器左边框架的 Domains（域名）下看到 xpc.edu.cn 项，其下的 Users（用户）中就包含了一个名为 Anonymous 的账户，此账户登录后的虚拟根目录（主目录）即为 D:\ftpserver/anon 目录。如图 10.21 所示。

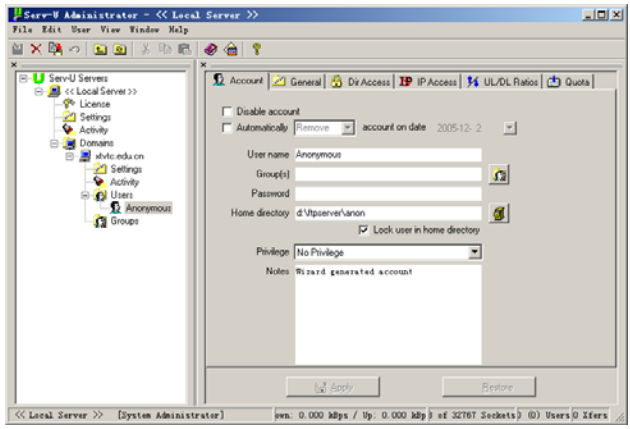

图 10.21　配置完成界面

3．Serv-U的卸载

选择“开始→程序→Serv-U FTP Server”下的 Remove Serv-U（卸载），按提示操作即可。

4．Serv-U的汉化

从软件下载网站下载 Serv-U 的汉化包程序。注意，下载的 Serv-U 的汉化包程序要与安装的 Serv-U 版本号一致，然后运行汉化程序，并按提示进行安装。

5．Serv-U的配置

再次进入 Serv-U 主程序，在图 10.21 中，单击“Local Server→Settings”选项，进入 Serv-U

服务器的设置页面，这些设置对 Serv-U 下所有的 FTP 服务器都起作用。

➢ 在“General”选项中可以设置整个服务器的“最大上传速度”、“最大下载速度”，“最大用户数量”、“检查匿名密码”、“文件/目录只使用小写字母”，以及拦截 FTP_Bounce 攻击和自动锁定某些用户的 IP 地址等，可根据实际情况设置。

➢ 在“SSL Certificate”选项中显示了 Serv-U 使用的证书的信息。

➢ 在“Advanced”选项中可以设置 PASV 端口范围、文件上传和下载、超时等信息。

下面进行 xpc.edu.cn 站点的设置。

1）消息设置

选择“Domains→ xpc.edu.cn →Settings”命令，打开设置界面，如图 10.22 所示。选择“Messages”选项，在此设置所属 FTP 服务器，当有用户登录、注销、更改目录或 FTP 服务器没有响应设置时，返回给登录用户的消息。除“服务器响应消息”是一行信息外，其他都可以是一个提前编辑好的文本文件。

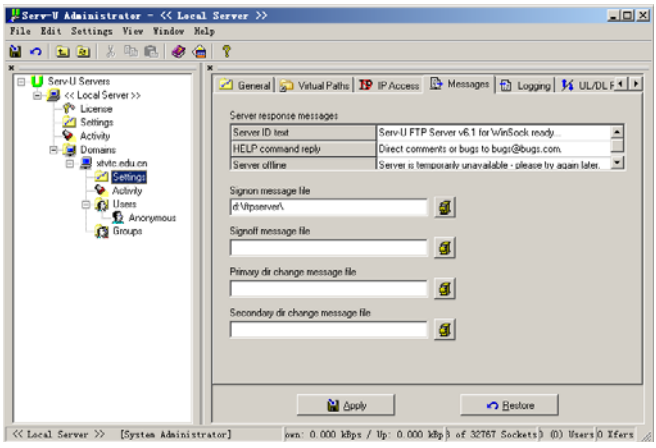

图 10.22　消息设置

2）用户和文件夹管理

① 选择“Domains→xpc.edu.cn→Users”选项，在右侧窗格中的空白处右击鼠标，从弹出的菜单中选择“new Users”命令，或按“Insert”键，弹出“Add New User→Step 1”对话框，在“user name”文本框中输入用户名，如“chujl”。

② 单击“Next”按钮，在“Add New User→Step 2”对话框中的“password”文本框中输入密码。

③ 单击“Next”按钮，在“Add New User→Step 3”对话框中的“user directory”文本框中输入该用户的文件夹，如“D:\ftpserver\wlzx”。

④ 单击“Next”按钮，在“Add New User→Step 4”对话框中选中“Yes”，单击“Finish”按钮。

按照以上步骤再创建 liuyf 用户，并让 D: \ftpserver\xxzx 文件夹作为 liuyf 的主目录。

3）为用户添加文件夹

当创建完用户后，每个用户只能访问自己的文件夹。如果需要用户访问其他分区或其他目录，就需要首先为用户添加文件夹。

① 选择“Domains→xpc.edu.cn→settings”选项，打开“virtual paths”选项，单击“virtual

path mappings”下的“Add”按钮。

② 在“Virtual Path Mappings→step 1”对话框的“physical path”文本框中输入“D:\ftpserver/pub”，或者单击“brower”按钮。

③ 单击“Next”按钮，在“Virtual Path Mappings→step 2”对话框的“map physical path to”文本框中输入“%home%”。%home%代表将 D:\ftpserver\pub 文件夹映射到当前 FTP 的所有用户主目录中。

④ 单击“Next”按钮，在“Virtual Path Mappings→step 3”对话框的“mapped path name”文本框中输入映射的路径的名称，如“pub”。单击“Finish”按钮，完成映射。

4）用户权限设置

默认情况下，每个用户只能对自己的主目录具有完全控制权，而对其他目录没有任何权限。

① 选择“Domains→xpc.edu.cn→users→anonymous”选项，打开“Dir Access”选项，单击“Add”按钮，在弹出的“add file/path to access rules”对话框中，输入“D:\ftpserver\pub”。

② 单击“Finish”按钮，为 D:\ftpserver\pub 在右侧选择默认权限，文件为“Read”、目录为“list”。如图 10.23 所示。

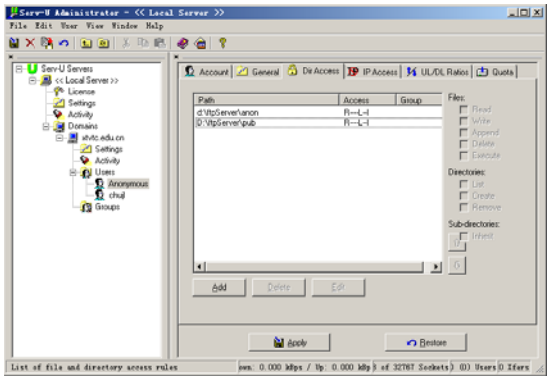

图 10.23　设置用户权限

③ 假设 chujl 对 D:\ftpserver\xxzx 和 D:\ftpserver\pub 文件夹有完全控制权限，则先选择 chujl 用户，在“Dir Access”选项卡中添加这两个文件夹，并为这两个文件夹添加除“excute”权限以外的所有权限即可。

5）用户的其他操作

对用户的其他操作包括禁用账户、修改密码、磁盘配额等。以 chujl 用户为例进行说明。

① 自动禁用账户和修改密码。在用户的“users”选项卡中，可以禁用账户、在指定日期禁用或删除账户，以及修改账户密码、更改账户的主目录、更改账户属性等。

② 登录设置。在“general”选项卡中，可以选择是否“需要安全连接”、是否“隐藏”文件、是否限制同一 IP 登录的数量、是否允许用户更改密码，还可以设置用户的最大上传和最大下载速度，以及该用户的登录消息文件等。

③ 限制用户使用磁盘空间。如果想限制用户使用的磁盘空间小大，需要在“配额”选项卡中进行设置。

习　题

一、名词解释

1．FTP　2. 匿名 FTP　3. TFTP

二、填空题

1．_____是 File Transfer Protocol 的缩写，是_____的简称，是网络计算机之间进行文件传输的协议，特别适合传送较大的文件。

2．FTP 的默认端口是_____，HTTP 的默认端口是_____。

3．FTP 是 TCP/IP 的一种具体应用，它工作在 OSI 参考模型的_____层。

4．在 FTP 中采用匿名登录的用户名是_____。

三、选择题

1．如果没有特殊声明，匿名 FTP 服务登录账号为（　　）。

A．User　　B．Anonymous

C．Guest　　D．用户自己的电子邮件地址

2．通过（　　）服务器，可以实现服务器和客户机之间的快速文件传输。

A．WWW　　B．DHCP

C．FTP　　D．Web

3．一个 FTP 站点，IP 地址是 192.168.1.100，端口是 2121，则客户端访问该站点时，在 IE 浏览器的地址栏中的完整输入应该是（　　）。

A．http://192.168.1.100

B．http://192.168.1.100:2121

C．ftp://192.168.1.100/2121

D．ftp://192.168.1.100:2121

4．下面说法正确的是（　）。

A．Web 站点的主目录和操作系统最好放在不同的分区中

B．服务器上同时有 Web 站点和 FTP 站点时，两个站点的主目录最好在同一分区

C．为了方便用户访问，Web 站点的主目录应该开放写入权限

D．为了方便用户访问，Web 站点的主目录应该开放目录浏览权限

四、思考题

1．简述 FTP 协议的工作原理。

2．FTP 命令如何使用？

3．TFTP 协议有何特点？用在什么地方？

4．下载文件的常用方法有哪些？

五、实训题

在天空软件园下载 Windows Server 2003 的补丁程序。

项目 11　电子邮件服务

全世界每天都有上千万的人在使用电子邮件，电子邮件已经成为人们生活中的一个重要部分，电子邮件（Electronic Mail，简称 E-mail）是因特网上最受欢迎也是最为广泛的应用之一，用户可以通过电子邮件与远程因特网用户进行经济、方便和快捷的信息交流。

11.1　项目内容

1．项目目的

在了解电子邮件的概念、格式、系统组成及工作原理的基础上，以 Windows Server 2003 操作系统为服务平台，掌握使用 WinWebMail 架设单位内部的邮件服务器，并进行管理，熟悉邮件系统的安全防护设置。

2．项目任务

有一所高等院校，组建了学校的校园网，为了便于老师之间的信息传递，需要架设 E-mail 服务器。

3．任务目标

① 了解电子邮件服务的基本原理；
② 熟练使用 WinWebMail 进行邮件服务器的配置和管理；
③ 学会邮件系统的安全防护设置。

11.2　相关知识

11.2.1　电子邮件的概念

电子邮件将邮件发送到 Internet 信息提供商（简称 ISP）的邮件服务器，并放在其中的收信人邮箱（mail box）中，收信人可随时上网到 ISP 的邮件服务器进行读取。相当于利用因特网为用户设立了存放邮件的信箱，E-mail 有时也称为“电子信箱”。因此，电子邮件服务是一种通过计算机网络与其他用户进行联系的快速、简便、高效、廉价的现代化通信手段。电子邮件之所以受到广大用户的喜爱，是因为与传统通信方式相比，具有以下优点：

- 快速、经济；
- 一件多发，即同时发给多个收件人；
- 除了可以发送简单的文本信息外，还可以附件形式发送各种多媒体文件。

与实时信息交流（如电话、传真）相比，电子邮件采用类似于传统邮件的“存储转发”机制，发送邮件时，并不需要收件人处于在线状态，收件人可根据需要随时上网从邮件服务器上收取邮件。

11.2.2 电子邮件的格式

电子邮件有自己规范的格式，电子邮件的格式由信封和内容两部分组成，即邮件头（header）和邮件主体（body）两部分。邮件头包括收信人 E-mail 地址、发信人 E-mail 地址、发送日期、标题和发送优先级等，其中，前两项是必选的。邮件主体是发件人和收件人要处理的内容，早期的电子邮件系统使用简单邮件传送协议（SMTP），只能传递文本信息，而通过使用多用途因特网邮件扩展协议 MIME (Multipurpose Internet Mail Extensions)，现在还可以发送语音、图像和视频等信息。对于 E-mail 主体不存在格式上的统一要求，但对信封即邮件头有严格的格式要求，尤其是 E-mail 地址。

E-mail 地址的标准格式为：<收信人信箱名>@主机域名

其中：

- 收信人信箱名指用户在某个邮件服务器上注册的用户标识，即代表收件人的账户名或邮箱名。
- @为分隔符，一般把它读为英文的 at。
- 主机域名是指信箱所在的邮件服务器的域名。一般可以将邮件主机名省略。

例如 chujl@263.net，表示在 263 在线的邮件服务器上的用户名为 chujl 的用户信箱。

11.2.3 电子邮件系统的组成

有了标准的电子邮件格式，电子邮件的发送与接收还要依托由邮件用户代理、邮件服务器和邮件协议组成的电子邮件系统。图 11.1 是电子邮件系统的简单示意图。

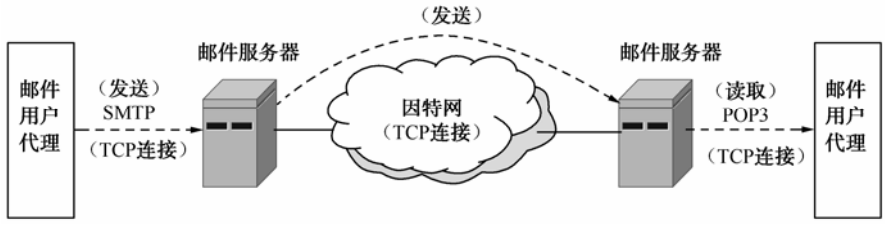

图 11.1　电子邮件系统的组成

1．邮件用户代理

邮件用户代理 MUA（Mail User Agent）就是用户与电子邮件系统的接口，在大多数情况下就是用户计算机中运行的程序。邮件用户代理为用户提供了一个很友好的接口，它可以提供命令行方式、菜单方式或图形方式的界面来与电子邮件系统交互，目前主要是窗口界面，允许人们读取和发送电子邮件，如 outlook express、hotmail、Foxmail，以及基于 Web 界面的用户代理程序等。用户代理至少应当具有撰写、显示、处理三个基本功能。

（1）撰写。给用户提供很方便地编辑信件的环境。如应让用户能创建便于使用的通信录，回信时具有回复等功能。

（2）显示。能方便地在计算机屏幕上显示邮件（包括邮件附件中的声音和图像）。

（3）处理。能够发送邮件和接收邮件。

2．邮件服务器

邮件服务器是一种用于存储和转发电子邮件的服务器端应用程序。邮件服务器是电子邮

件系统的核心构件，包括邮件发送服务器和邮件接收服务器，邮件服务器按照客户/服务器模式工作。邮件发送服务器是指为用户提供邮件发送功能的邮件服务器，如图 11.1 的 SMTP 服务器；邮件接收服务器是指为用户提供邮件接收功能的邮件服务器，如图 11.1 中的 POP3 服务器。

3．邮件协议

用户在发送邮件时，要使用邮件发送协议，常见的邮件发送协议有简单邮件传输协议 SMTP（Simple Mail Transfer Protocol）和多用途因特网邮件扩充协议 MIME。前者只能传输文本信息，而后者则可以传输包括文本、声音、图像等在内的多媒体信息。当用户代理向电子邮件发送服务器发送电子邮件时，或邮件发送服务器向邮件接收服务器发送电子邮件时，都要使用邮件发送协议。用户从邮件接收服务器接收邮件时，要使用邮件接收协议，通常使用邮局协议 POP3（Post Office Protocol），该协议由 RFC1225 定义，具有用户登录、退出、读取消息、删除消息的命令。POP3 的关键之处在于其能从远程邮箱中读取电子邮件，并将它存在用户本地的机器上以便以后读取。通常，SMTP 使用 TCP 的 25 号端口，而 POP3 则使用 TCP 的 110 号端口。

11.2.4　电子邮件的邮递机制

图 11.2 给出了一封电子邮件发送和接收的整个过程。假定用户 XXX 使用“XXX@sina.com.cn”作为发信人地址向用户 YYY 发送一个文本格式的电子邮件，该发信人地址所指向的邮件发送服务器为 smtp.sina.com.cn，收信人的 E-mail 地址为“YYY@263.net”。

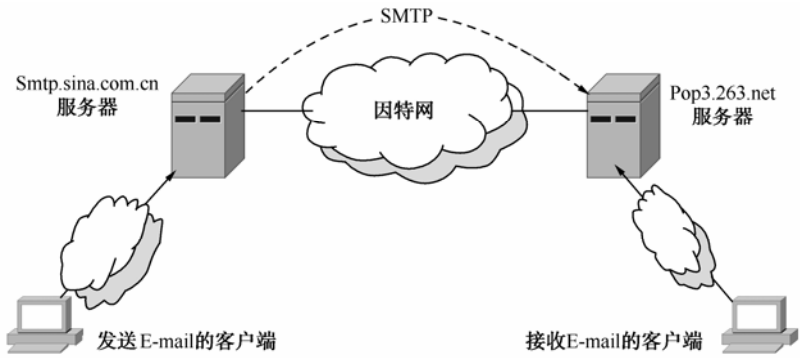

图 11.2　电子邮件发送和接收实例

首先，用户 XXX 在自己的计算机上使用独立式的文本编辑器、文字处理程序或用户代理内部的文本编辑器来撰写邮件正文，然后，使用电子邮件用户代理程序如 outlook express 完成标准邮件格式的创建，即选择创建新邮件图标，填写收件人地址、主题、邮件的正文、邮件的附件等。

一旦用户选择邮件发送图标之后，则“用户代理程序”将用户的邮件传给负责邮件传输的程序，由其在 XXX 所用的主机和名为 smtp.sina.com.cn 的发送服务器之间建立一个关于 SMTP 的连接，并通过该连接将邮件发送至服务器 smtp.sina.com.cn。

发送方服务器 smtp.sina.com.cn 在获得用户 XXX 所发送的邮件后，根据邮件接收者的地址，在发送服务器与 YYY 的邮件接收服务器之间建立一个 SMTP 的连接，并通过该连接将

邮件送至 YYY 的接收服务器。

当邮件被送到邮件交换服务器（SMTP Server）后，邮件交换服务器必须将邮件转发到目的地的邮件交换服务器，邮件交换服务器向 DNS 服务器查找 MX 资源记录来得知目的地的邮件交换服务器。MX 记录着负责域邮件传送的交换服务器，如图 11.3 所示。

接收方邮件服务器 pop3.263.net 接收到邮件后，根据邮件接收者的用户名将邮件放到用户的邮箱中。在电子邮件系统中，为每个用户分配一个邮箱（用户邮箱）。例如在基于 UNIX 的邮件服务系统中，用户邮箱位于/usr/spool/mail/目录下，邮箱标识一般与用户标识相同。

当邮件到达邮件接收服务器后，用户随时都可以接收邮件。当用户 YYY 需要查看自己的邮箱并接收邮件时，其首先要在自己的计算机与邮件接收服务器 pop3.263.net 之间建立一条关于 POP3 的连接，该连接也是通过系统提供的“用户代理程序”进行。连接建立之后，用户就可以从自己的邮箱中“取出”邮件进行阅读、处理、转发或回复等操作。

电子邮件的“发送→传递→接收”是异步的，邮件发送时并不要求接收者正在使用邮件系统，邮件可以存放在接收用户的邮箱中，接收者随时可以接收。

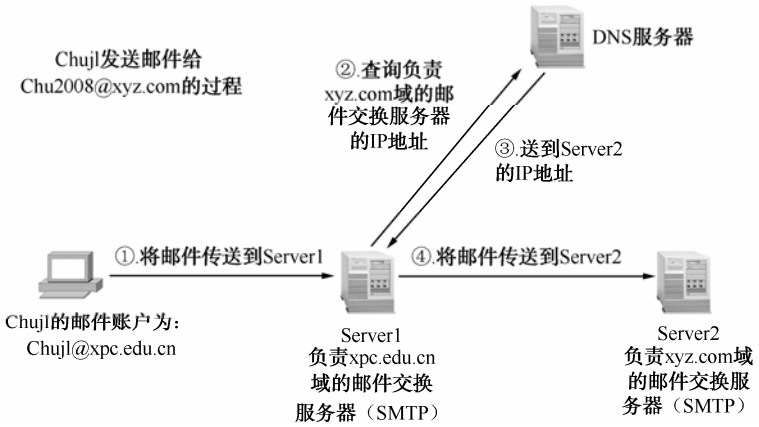

图 11.3　查找目的地邮件服务器的过程

11.2.5　邮件服务器的类型

在 Internet 或 Intranet 上构建电子邮件服务，一般需要建立两种服务器，即邮件发送服务器（一般采用 SMTP 协议）和邮件接收服务器（根据所用协议的不同，可分为 POP3 服务器和 IMAP4 服务器）。

1．SMTP服务器

SMTP 是简单邮件传送协议，当在两个邮件服务器之间建立直接连接以及从邮件客户端发送邮件时使用。电子邮件就是通过 SMTP 服务器发送出去的。SMTP 是一个在服务器之间传递邮件的协议，能将一个 SMTP 服务器上的邮件转发到另一个 SMTP 服务器。SMTP 是一个单向协议，只能发送，不能接收。SMTP 协议的标准 TCP 端口为 25。

2．POP3 服务器

当邮件到来后，首先存储在邮件服务器的电子信箱中。如果用户希望查看和管理这些邮件，可以通过 POP3 协议将邮件下载到用户所在的主机。

POP3 是邮局协议（POP）的第 3 代版本，它允许用户通过计算机动态检索邮件服务器上

的邮件。POP3 只是对邮件服务器上的邮件提供下载和删除等功能。

POP3 本身采用客户/服务器模式，其客户程序运行在接收邮件的用户计算机上，POP3 服务器程序运行在其 ISP 邮件服务器上。从网上收到的邮件是根据收信人的邮件地址交付给目的 ISP 邮件服务器，而收信人用计算机不定期地连接到这个邮件服务器以便将发送给他的邮件下载到其计算机上。此后，所有对邮件的处理都在用户的计算机上进行。POP3 服务器是一个具有存储转发功能的中间服务器。一旦邮件交付给用户的计算机，POP3 服务器就不再保存这些邮件（也可以设置保留备份）。用户在取回邮件并中断与 POP3 服务器的连接后，可在自己的计算机上处理收到的邮件。因此，POP 实际上是一个脱机协议。POP3 协议的标准 TCP 标准端口为 110。

3．IMAP4 服务器

IMAP 是因特网报文存取协议（Internet Message Access Protocol），现在较新的是版本 4，即 IMAP4，它同样采用客户/服务器模式。在 IMAP 时，所有收到的邮件同样先送到 ISP 邮件服务器的 IMAP 服务器。而在用户的计算机上运行 IMAP 客户程序，然后与 ISP 邮件服务器的 IMAP 服务器程序建立 TCP 连接。用户在自己的计算机上就可以操纵 ISP 的邮件服务器的邮箱，就像在本地操纵一样，因此，IMAP 是一个联机协议。当用户计算机上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，用户就可看到邮件的首部。若用户需要打开某个邮件，该邮件才会传到用户的计算机上。用户可以根据需要为自己的邮箱创建便于分类管理的层次式的邮箱文件夹，并且能够将存放的邮件从某一个文件夹移动到另一个文件夹中。用户也可按某种条件对邮件进行查找。在用户未发出删除邮件的命令之前，IMAP 服务器邮箱中的邮件一直保存着。IMAP 可以让用户在不同的地方使用不同的计算机随时阅读和处理自己的邮件。

11.2.6 Web邮件服务

将电子邮件服务集成到 Web，可以让用户非常方便地通过浏览器来完成申请邮箱、撰写邮件和收发邮件等操作。目前 Internet 上许多电子邮件服务都提供 Web 邮件服务，如网易、搜狐、雅虎、263 等。

Web 邮件（Web mail）服务是将电子邮件服务集成于 Web 来实现的。按功能可以分为两类，一是面向管理员，提供管理邮件服务器的 Web 服务，管理员可以通过浏览器来管理邮件服务器；二是面向普通用户，提供收发邮件的 Web 服务，可以通过浏览器收发邮件。

11.2.7 邮件服务器软件的选择

目前，邮件服务器软件非常丰富，如 Netscape Messaging Server、Lotus Notes /Domino、Microsoft Exchange Server、Sendmail、VPOP3、MDaemon Server、WebEasyMail 等，其中后 4 个软件是免费的。

Netscape Messaging Server 是 Netscape 组件中的邮件服务系统，一般被用做邮件服务 Engine，是邮件服务器的核心部分，以它来管理邮件队列、邮件协议服务等，是目前流行的邮件服务器软件。

Lotus Notes/Domino 是莲花公司推出的邮件服务器软件产品。Domino 是指服务器，Notes 是指客户端软件。用户安装完 Lotus Notes/Domino 后，不用做更多的开发，即可在单位内部架构强大的邮件系统。

Sendmail 是一个具有高弹性及高设定度的邮件传送代理（Mail Transfer Agent, MTA）。最早开发 Sendmail 的是 Eric Allman。这个软件功能强大、可靠并具有可伸缩性，是一个非常优秀的软件。

Exchange Server 是美国微软公司开发的，能满足各种规模的商务活动（从小型组织到最大型的分布式企业）的 通信和协作需要。Exchange与其客户端Microsoft Outlook一起，提供了一个具有高可靠性、可升级性且易于管理的通信和协作基础架构。

VPOP3 邮件网关，可从 POP3 帐号收信，然后根据用户自设的过滤条件将信件分配到多个指定的局域网 POP3 信箱，等待局域网用户取信。该软件支持 POP3、SMTP 和 LDAP 协议，且该电子邮件服务器软件拥有一个内置的 WebMail 服务。

MDaemon Server 是一款优秀的全功能专业邮件服务器软件，它支持 SMTP、POP3、IMAP 和 MIME 邮件服务。

WebEasyMail 通过与微软 IIS（Microsoft Internet Information Services）的紧密集成，提供 Web 下系统管理，以及通过浏览器收、发电子邮件等功能，提供了 14 个对象，百种方法及属性，以支持高级用户针对 WebEasyMail 系统所进行的相关 ASP 程序开发。

11.3 方案设计及准备

1．设计

在学院的校园网上，在一台安装 Windows Server 2003 操作系统的服务器上，使用 WinWebMail 架设单位内部的邮件服务器，并开设账户，实现 E-mail 邮件传送的功能。网络拓扑图如图 11.4 所示。

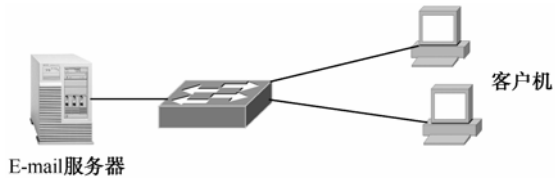

图 11.4 E-mail 网络拓扑图

2．设备清单

为了搭建图 11.4 所示的网络环境，需要下列设备：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 安装 Windows XP 的计算机 2 台；

③ 以上两台计算机已连入校园网。

11.4 项目实施

WinWebMail，原名为 WebEasyMail，是一个基于 Windows 平台，并服务于中、小型网站及企业的 Internet（英特网）和 Intranet（企业局域网）全功能、安全高速 Web 邮件服务器软件，支持 WebMail、POP3、SMTP、IMAP4、CA Server、TLS/SSL 等协议，同时具备网络

硬盘存储、讨论组、电子邮件病毒扫描、垃圾邮件拦截引擎、数字证书服务、数字签名、数字加密等功能，全面支持 Web 管理功能，提供企业级邮件服务器解决方案。WebEasyMail 通过与 IIS 的紧密集成，提供 Web 下的系统管理以及通过浏览器收、发电子邮件等功能。

步骤 1：安装WinWebMail

WinWebMail 的安装比较简单，在网上下载该软件后，直接运行安装文件，不需要任何选项，就可以完成安装。安装完成后，会在桌面上生成一个 WinWebMail 快捷图标。双击该快捷图标运行 WinWebMail，就会在状态栏生成一个缩略图。

在运行 Win Web Mail 之前，需要卸载用微软的 SMTP 服务，否则会发生端口冲突。

步骤 2：设置DNS地址

DNS 地址的设置非常重要，将直接影响对外网（因特网）发送邮件的成败。设置的 DNS 服务器如果停止工作或无法连接，会造成大量待发送邮件。

运行 WinWebMail，在 Windows 状态栏上有一个 WinWebMail 图标，用鼠标右击该图标，并选择“服务”选项，弹出“WinWebMail 服务”对话框，如图 11.5 所示。设置首选和备用 DNS 的 IP 地址。

（1）选中“修改”才可以对 DNS 进行修改。

（2）首选 DNS 的 IP 地址：此项不可为空且输入的 DNS 地址必须是有效的，才可以向因特网发信，有效的 DNS 服务器地址可以从 ISP 服务商处询问到。

（3）备用 DNS 的 IP 地址：强烈建议填写此项，并需确保有效且与首选 DNS 地址不同。如果首选 DNS 服务器出错或停止服务，WinWebMail 将会自动使用备用 DNS 地址发信，从而保证通信畅通。

（4）启用“当 DNS 查询 MX 记录失败，从 DNS 根服务器查询”项：可以提高邮件发送的成功率，当使用邮件系统指定的 DNS 地址查询 MX 记录失败后，将从 DNS 根服务器进行查询。单击“设置”按钮，弹出“DNS 根服务器”对话框，如图 11.6 所示。

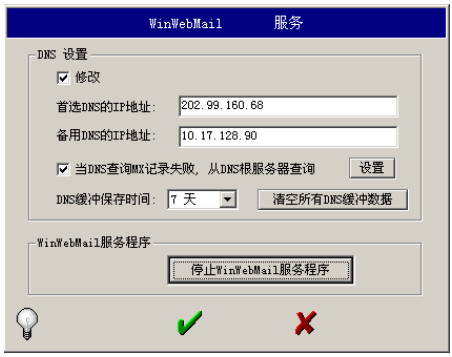

图 11.5 “WinWebMail 服务”对话框

图 11.6 “DNS 根服务器”对话框

可以添加互联网的 DNS 根服务器，也可以直接添加其他一些高性能的 DNS 服务器 IP 地址。

DNS 根服务器地址列表。除根服务器外，建议填写 IP 地址，如：

m.gtld-servers.net

b.gtld-servers.net

j.gtld-servers.net

205.252.144.228

a.gtld-servers.net

（5）“DNS 缓冲保持时间”：在邮件服务器上保存 MX 记录的时间。

（6）单击“清空所有 DNS 缓冲数据”按钮，可以消除所有保存在邮件服务器上的 MX 记录缓存。

（7）停止或启动 WinWebMail 服务程序。注意：当按钮显示为“停止 WinWebMail 服务程序”时，即表示当前服务程序已经启动，而当按钮显示为“启动 WinWebMail 服务程序”时，表示当前服务程序已经停止。

在大部分情况下，对外部（因特网）邮箱发信失败都是因为 DNS 设置不当或所使用的 DNS 无法正常工作引起的。

可以使用下面这些 DNS 地址，或直接询问本地 ISP 服务提供商：

205.252.144.228

202.106.127.1

216.2310.32.10

168.95.1.1

202.106.0.20

202.102.192.68

202.96.1910.133

为了确保所选用的 DNS 可以正常使用，可以在服务器上 ping 该 DNS 地址，当可以 ping 通时，即可以认为该 DNS 能够正常工作。请优先选择响应时间最短的 DNS，因为这样将可以大幅提高外发邮件的速度。

更改 DNS 地址后，需要重启 WinWebMail 服务程序才能生效。

因为邮件系统对外发信时需要和 DNS 服务器就目标邮件服务器的地址解析，进行 UDP 通信，所以必须允许 UDP 包通过，如果出于安全原因要封闭 UDP 端口，那么也必须开放 1024 以上的 UDP 端口。

WinWebMail 的服务程序是 emsvr.exe 文件，可以在系统进程中查看到。服务程序的注册和注销命令，

注册命令：

[完整路径]\emsvr.exe -reg

注销命令：

[完整路径]\emsvr.exe -unreg

步骤 3：设置域名

域名设定就是设定用户邮件“@”号后的域名，系统默认域名为：system.mail，当在此域名下添加了一个新的用户，如用户名为：winwebmail，则该用户在 WinWebMail 邮件服务器上的默认邮件地址为：winwebmail@system.mail

system.mail 域是系统保留域名，此域名不可删除，虽然可以不在该域中放置任何用户。也可以用管理员身份通过浏览器登录 WebMail 系统，然后在“系统设置”的“域名控制”中将此域名隐藏起来。

用鼠标右击 Windows 状态栏上的 WinWebMail 图标，并选择“域名管理”选项，弹出“WinWebMail 域名管理”对话框，单击工具栏上的“添加”按钮，并在文本框中输入域名，如 xpc.edu.cn，然后单击“确定”按钮添加域名，如图 11.7 所示。

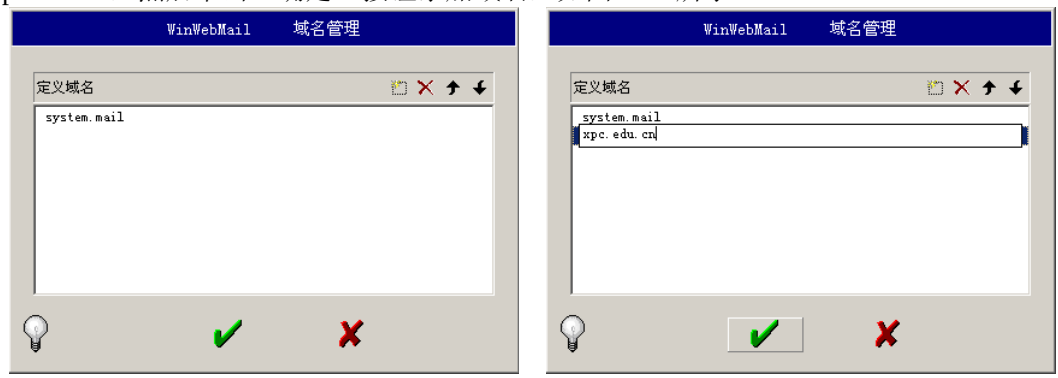

图 11.7　添加 WinWebMail 域名

步骤 4：**授予用户访问权限**

WinWebMail 安装目录及根目录的用户权限设置很重要，例如，WinWebMail 被安装在 D:\WinWebMail 目录下。权限设置完成后，需要重启 IIS 以使设置生效见表 11.1。

表 11.1　WinWebMAIL 目录及用户权限

目　录	用　户	权　限
D:\WinWebMail (及其所有子目录)	Users 或 Everyone	完全控制
	Administrators	完全控制,继承的
	System	完全控制,继承的
	匿名账号	完全控制
	IIS_WPG	读取写入
D:\根目录	Users	读取
	Administrators	完全控制
	System	完全控制
	匿名账号	读取运行
	IIS_WPG	只有根目录是读取运行,不继承

步骤 5：WinWebMail用户管理

管理邮件系统中的用户数据。用鼠标右击 Windows 状态栏上的 WinWebMail 图标，并选择“系统设置”选项，弹出“WinWebMail 系统设置”对话框，如图 11.8 所示。默认为“用户管理”选项卡。

输入用户名（如 user1）及密码，并从“域”下拉列表中选择“xpc.edu.cn”，然后单击“添加”按钮添加账户。

用同样的办法添加用户 user2、user3 等用户。

（1）禁用账号：账号禁用后此用户依然在系统中，但他将无法通过 POP3/IMAP4/WebMail 渠道接收邮件（快捷键：Alt+F）。

（2）设置允许该账号访问系统的方式（由 HTTP、SMTP、POP3、IMAP4 4 种访问方式

进行组合）。

（3）最后登录日期，用户最近一次访问 POP3、IMAP4 或 WebMail 的日期，当账号被禁用时，此时间将会被更改为账号禁用的日期。

（4）可设置用户账号的到期日期，在所设置的日期到达后，该用户账将会被系统自动禁用。

（5）提供针对单个用户的高级设置选项。如系统中任一个用户有多个因特网信箱需要接收邮件，而他希望能通过本地邮件服务器将因特网上的多个邮箱里的邮件接收到本地，然后再一次性下载所有的邮件时，就需要使用本项中的设置了。选择一个用户（如 user1），单击“高级”按钮，弹出“[user1] 的 POP 接收代理设置”对话框，如图 11.9 所示。

图 11.8　用户管理

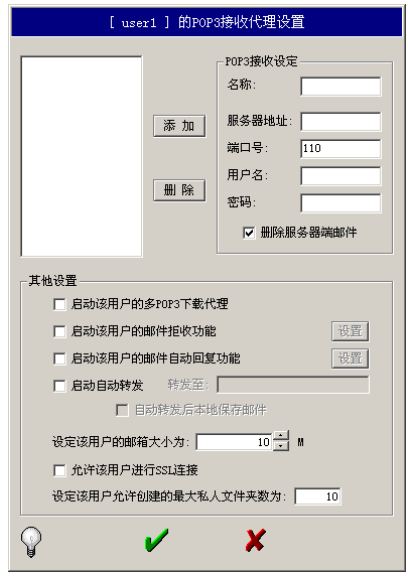

图 11.9　POP 接收代理设置

① 在“POP 接收设定”选项组可以设置：

➢ POP3 接收的显示名称（只是用来显示，可输入任意内容）。

➢ 设定需下载的 POP3 邮箱服务器的地址（可以是 IP 地址，如：202.104.32.234。也可以是字符串地址，如：pop.21cn.com）。

➢ 选中“删除服务器端邮件”复选框，表示下载邮件后删除服务器端的邮件。

把输入的数据加入到 POP3 接收列表中，只有加入接收列表的数据才是有效的。

② 只有选中“启动该用户的多 POP3 下载代理”复选框多 POP3 接收服务才启动。

③ 选中“启动该用户的邮件拒收功能”，单击“设置”按钮，弹出“[user1] 的拒收邮件列表”对话框，如图 11.10 所示。

用户可以拒收来自特定邮件发件人所发的邮件（支持通配符方式）。

通配符说明：

➢ *：任意长度的任何内容。

➢ ?：一个字符的任何内容。

如图 11.10 中第一行的 someone*bad@*.*，此时将拒收来自如 someoneAbad@china.com 或是 someoneBCDEFbad@163.net 的邮件。

如图 11.10 中第二行的 b??@yahoo.???，此时将拒收来自如 bAB@yahoo.com 或是 b06@yahoo.net 的邮件。

④ 选中“启动该用户的邮件自动回复功能”，单击“设置”按钮，弹出“[user1] 的自动回复邮件内容设置”对话框，如图 11.11 所示。

图 11.10　拒收邮件列表设置

图 11.11　自动回复邮件内容设置系统的组成

当用户设定自动回复邮件内容，并在“高级设定”中启用了此功能后，它将会以此内容自动回复所有来信。当设置有效期后，将只在有效期内才进行邮件自动回复。

- 设置有效期的起始日期。
- 设置有效期的结束日期。
- 输入自动回复邮件的主题。注意：不可为空。
- 输入自动回复邮件的内容。

⑤ 选中“启动自动转发”选项，然后在“转发至”文本框中输入要转发到的邮件地址。

⑥ 设定该用户的邮箱大小，输入数值即可。

步骤 6：WinWebMail系统邮件

在图 11.8 中选中“系统邮件”选项卡，打开“系统邮件管理”对话框，如图 11.12 所示。设置各类系统邮件的主题和内容。

（1）邮件发送失败后的回复信。当邮件发送失败时（比如超期发送），系统将会自动回复一封邮件给发件人，告诉他此邮件投递失败。此设置项用来设定系统回复邮件的主题和内容（注意：原邮件内容的前 100 行信息将会被附在自动回复邮件的尾部）。

- %errmail%：将会被填充为发送失败的邮件地址信息及失败原因。

（2）致新用户邮件。当创建新用户后，设置将发送给此用户的欢迎信的主题和内容。

（3）邮件读取（下载）确认信。此项功能应用于 WebMail，当系统内用户间通信时可选用此功能，这样当收件人（系统内用户）通过

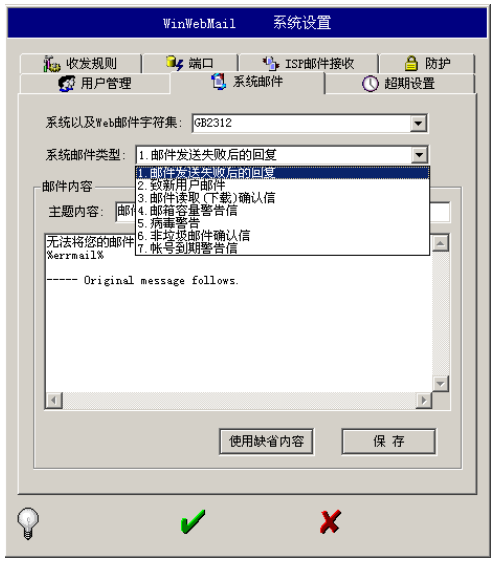

图 11.12　系统邮件管理

WebMail 看信或是通过 POP3、IMAP4 下载邮件时，原发件人（系统内用户）将收到一封回执。

- %to%：将会被填充为原发件人的邮件地址。
- %sendtime%：将会被填充为原发件人发信的时间。
- %from%：将会被填充为收件人的邮件地址。

（4）邮箱容量警告信。当用户的邮箱快要满时，系统将会发信给用户提醒他及时清理邮箱。

（5）病毒警告信。在启用相关的邮件防病毒功能后，系统发现接收到的邮件带有病毒时，将自动回复发信方的内容。

- %VirusName%：将会被填充为病毒名称。

（6）非垃圾邮件确认信。在 IE 浏览器中启用相关防垃圾邮件功能后，用户邮箱在收到一封不明邮件时将会先放置到垃圾箱中，然后向发信方自动发送一封邮件，要求原发信方计算一道随机生成的数学加法题目后，将答案填写到主题中并回复。当系统接收到正确的答案后才会将原邮件转到用户的收件箱中。

- %question%：将会被填充为需要回答的问题内容。（重要）
- %date%：将会被填充为当前日期。
- %time%：将会被填充为当前时间。
- %sendname%：将会被填充为发件人名称。
- %sendmail%：将会被填充为发件人邮件地址。
- %subject%：将会被填充为来信的标题。

（7）账号到期警告信。此功能可以在账号即将过期前，向该账号发送警告信。

- %ExpDate%：将会被填充为账号到期日期（YYYY-MM-DD）。
- %RemDays%：将会被填充为距离账到期的天数。
- %ExpAccount%：将会被填充为被警告的账号名称。

（8）垃圾箱邮件统计信。此功能可以对用户垃圾箱内的邮件进行统计，并可经由 POP3 协议下载到客户端。需要修改第一行 %URL%后的内容为邮件系统可以由外部访问的 HTTP 地址，并且最后需要由 /trashmsg.asp 结尾。例如，http://www.domain.com/mail/trashmsg.asp 或 http://mail.domain.com/trashmsg.asp

- %Account%：将会被填充为用户账号名称。
- %Email%：将会被填充为用户邮件地址。
- %EmailsTotal%：将会被填充为垃圾箱中的邮件总数。

步骤 7：WinWebMail超时设置

设置系统尝试投递普通邮件及错误回复邮件的期限。当在“邮件超期设定”选项组中限定的期限内无法将此邮件成功发送，系统将自动回复该发信人，说明邮件发送失败（发送内容的定制）。在“系统回复邮件设定”选项组中设置此封错误回复邮件的发送期限，如在此期限内无法正确发送，该邮件将被系统删除。在图 11.8 中选中“系超时设置”选项卡，打开超时设置管理对话框，如图 11.13 所示。.

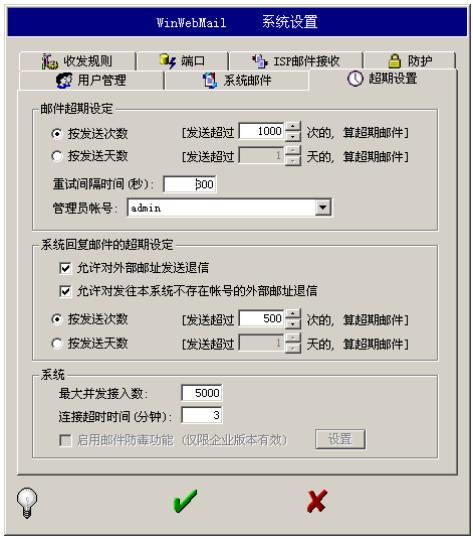

图 11.13　超时设置

（1）在“邮件超期设定”选项组。当一封普通邮件发送次数超过 10 次后，系统将认为发送失败，然后回复此邮件的发信人。一般设置在 5～500 之间。

当一封普通邮件发送天数超过 1 天后，系统将认为发送失败，然后回复此邮件的发信人。（不建议选用）

发送重试间隔时间，在队列中的邮件等待多长时间后被重新发送。

设置系统管理员账号。此账号将负责接收各类无法处理的投递失败邮件（默认为 admin）。（系统管理员将负责投递“新用户欢迎信”及“错误回复邮件”等系统邮件）

（2）在“系统回复邮件的超期设定”选项组。设置因为发送失败而自动回复邮件的尝试发送期限。当系统外地址发送邮件失败时，是否允许发送退信。

当系统外地址发送邮件到本系统不存在的账号时，是否允许发送退信。（因为病毒邮件以及垃圾邮件通常会对系统内不存在的地址发送邮件，所以一般情况下建议用户禁止此项功能，以避免大量的无用退信占用网络资源并可防止反垃圾邮件组织将退信误判为垃圾邮件后封闭 IP 地址）。

当错误回复邮件的发送次数超过 5 次后，系统将认为发送失败并删除邮件。一般设置在 3～100 之间。

当错误回复邮件的发送天数超过 1 天后，系统将认为发送失败并删除邮件。（不建议选用）

（3）在“系统”选项组。设置最大并发接入数。较大的并发接入数会提高性能，但会占用更多的内存。注意：此项设置需要重新启动服务程序后才能生效。

设置 SMTP/POP3/IMAP4 连接的不响应超时时间。

步骤 8：WinWebMail收发规则

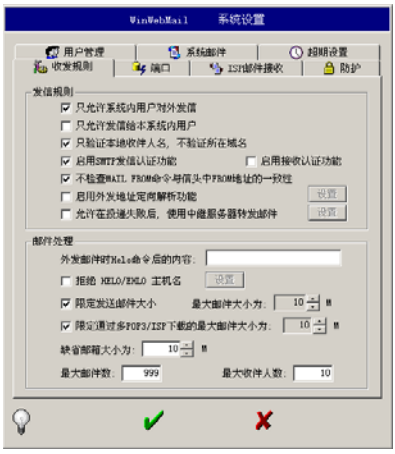

图 11.14　收发规则

在图 11.8 中选中“收发规则”选项卡，打开“收发规则管理”对话框，如图 11.14 所示。.

.1）在“发信规则”选项组

（1）启用“只允许系统内用户对外发信”功能后，将只允许本系统内用户通过 SMTP 协议对系统内以及系统外（因特网）投递电子邮件，非本系统内用户只允许通过 SMTP 协议对系统内发信。作为最基本的防垃圾邮件设置，强烈建议启用此功能。

用户可以通过在邮件客户端软件（如：Outlook Express）中的“用户信息”中的“电子邮件地址”处填写系统内有效账号所对应的邮件地址来通过此项验证。

判断是否是系统内用户将根据 SMTP 应答中 mail from

的地址进行识别。此选项不限制通过本系统 WebMail 发送的电子邮件。

（2）启用“只允许发信给本系统内用户”功能后，将只允许通过 SMTP 协议对系统内发信，而禁止任何用户通过 SMTP 协议对系统外（因特网）发信。此选项不限制通过本系统 WebMail 发送的电子邮件，即在启用此功能后，用户仍可以通过 WebMail 发送电子邮件到系统内或系统外（因特网）。

（3）用户存在于所有域名中。通过使用此功能可以实现当系统内有多个域名时，如 111.com、222.com、333.com，将所有发往 user@111.com 或 user@222.com 或 user@333.com 的邮件都发到一个账号：user 的邮箱内。注意：此选项不支持含域名的账号。

（4）选中“启用 SMTP 发信身份认证”功能后，将可以有效防范非系统内用户试图使用邮件服务器（通过 SMTP 协议）对外发送垃圾邮件。

SMTP 发信身份认证功能只针对外发（因特网）邮件，对系统内发信则无须进行身份认证。作为有效的防垃圾邮件设置，建议启用此功能。此选项不限制通过本系统 WebMail 发送的电子邮件。

（5）选中“启用接收认证功能”后，系统内账号通过 SMTP 协议互相发信时，将需要进行身份认证。

（6）是否检查 MAIL FROM 命令与信头中 FROM 地址的一致性。如果使用检查一致性的功能会拒收部分正常邮件，比如来自其他邮件服务器的自动转发邮件。

（7）定向解析系统外发邮件时的地址（设置外发地址定向解析）。可以应用在一个专网内有几台不同的邮件系统，各邮件系统使用不同的域名，并且没有进行 DNS 解析的情况。此功能也可以作为简单的外发邮件中继服务器进行设定。

（8）启用“允许在投递失败后，使用中继服务器转发邮件”功能后，邮件发往目标服务器失败时，系统将会使用所设置的中继服务器转发邮件。单击“设置”按钮，弹出“中继服务器”对话框，如图 11.15 所示。

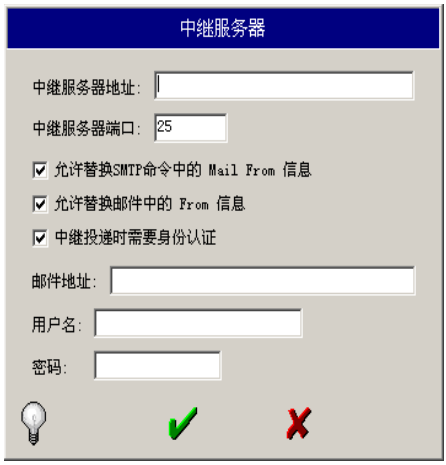

图 11.15 “中继服务器”对话框

- 中继服务器地址：输入中继服务器的 IP 地址。
- 中继服务器端口：中继服务器的 SMTP 服务所用端口，默认为 25。
- 选中“允许替换 SMTP 命令中的 Mail From 信息”功能后将 SMTP 命令中的 Mail From 信息替换为中继设置中的邮件地址信息。
- 选中“允许替换邮件中的 From 信息”功能后将中继发送邮件内容中的 From 信息替换为中继设置中的邮件地址信息。
- 选中“中继投递时需要身份认证”。如果中继服务器发信时需要身份认证，必须启用此功能。
  - 邮件地址：中继发送时的完整邮件地址。
  - 用户名：中继发送时的用户账号名称。
  - 密码：中继发送时的用户密码。

2）在“邮件处理”选项组

（1）“外发邮件时 Hello 命令后的内容”：表示 SMTP 命令应答过程中，HELO/EHLO 用的主机名。空白表示使用发信邮件地址中的域名。如果服务器上有多个域，可以填写一个已被正确解析的邮件域名，如 domain.com。

域名(如 domain.com) 做了 MX 记录时(如 MX 记录为 mail.domain.com)，可以设置 HELO 为该 MX 记录(如: mail.domain.com)。

域名(如 domain.com) 未做 MX 记录时，可以设置 HELO 为域名(如 domain.com)。

（2）选中“拒绝 HELO/EHLO 主机名”：如果用户不想接收动态域名主机发过来的邮件，可以填写动态域名到列表中来过滤动态域名发过来的邮件。单击“设置”按钮，弹出“拒绝 HELO/EHLO 主机名”对话框，如图 11.16 所示，单击“添加”按钮，输入要拒绝的 HELO/EHLO 主机名。

图 11.16　拒绝 HELO/EHLO 主机名

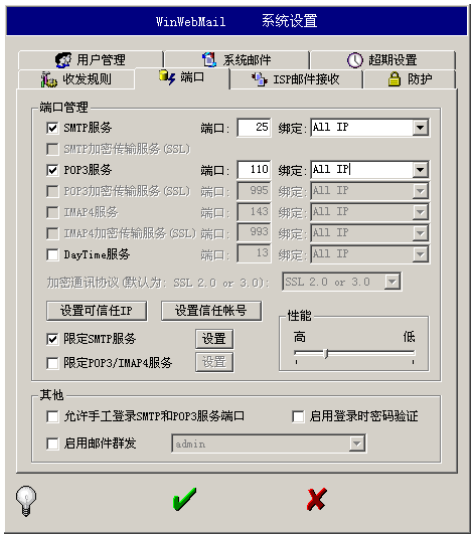

图 11.17　“端口”对话框

（3）缺省邮箱大小为：创建新账号时或没有特别指定邮箱大小时的缺省邮箱大小。此设置不可以修改现有用户的邮箱大小。

（4）最大邮件数：限定邮箱中的最多邮件数量（包括存储文件夹中的文件数量）。当用户的邮箱空间已被用完或者邮箱中的邮件（包括存储文件夹中的文件）数量达到此限定值时，系统会认为邮箱已满。

（5）最大收件人数：限定通过 SMTP 协议发送邮件时的最大收件人数。一般情况下所设置的值不应该超过 20。

步骤 9：WinWebMail端口

管理邮件系统中一些服务的启动与端口及速度引擎设置，并可进行群发邮件的设置。在图 11.8 中选中“端口”选项卡，打开“端口”对话框，如图 11.17 所示。

（1）在“端口管理”选项组：可以设置 SMTP 服务、POP3 服务等的端口号，以及绑定 IP。

（2）单击“设置可信任 IP”按钮，弹出“设置可信任 IP”对话框，如图 11.18 所示，可

以设置系统可信任 IP 地址集。可以通过输入 IP 地址或 IP 段（如：61.121.*）的方式来设置某些 IP 是可信并不受限制的。

（3）单击“设置信任账号”按钮，弹出“设置信任账号”对话框，如图 11.19 所示，设置系统可信任账号集。通过设置信任账号，可以让系统内的某些账号拥用更大的发信权限，如这些账号将不受外发邮件数量限制等。

图 11.18　“设置可信任 IP 地址”对话框

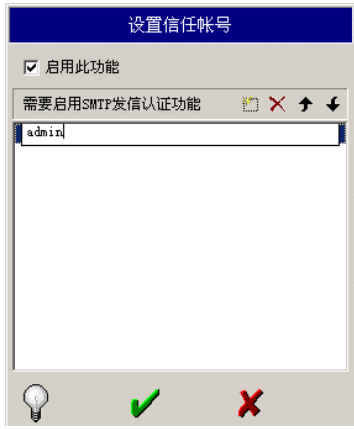

图 11.19　“设置信任账户”对话框

（4）启用限定 SMTP 服务的功能。建议非特殊需要无须使用此功能。

（5）设置允许使用 SMTP 服务的 IP 地址范围。

（6）启用限定 POP3/IMAP4 服务的功能。建议非特殊需要无须使用此功能。

（7）设置允许使用 POP3/IMAP4 服务的 IP 地址范围。

（8）速度引擎设置，可根据服务器的硬件性能动态调整 WinWebMail 的邮件处理速度。

（9）在“其他”选项组：

- 是否允许用户使用手工方式进行登录连接（如使用 telnet 工具）。注意：这种方式是低效的。
- 是否启用登录系统时的密码验证功能。注意：验证的是 admin 用户的密码。

图 11.20　ISP 邮件接收

- 是否启用邮件群发功能。它和邮件列表的区别在于：它是强制性的。启动此功能后无论是否使用了拒收功能，系统中所有用户（包括已禁用的用户）都将收到群发邮件。注意：这项功能的开启有可能会产生大量的废邮件，所以，建议在平时禁用此项功能，只当系统管理员需要使用群发功能时才开启，使用完毕后就应立即禁用此功能。
- 选定邮件群发账号。当发信到这个账号时，该邮件将会被发送至当前系统的所有信箱中。强烈建议管理选定一个很难猜到的账号作为邮件群发账号。

步骤 10：ISP邮件接收

如果公司有外部 ISP 邮箱，而想使局域网

内的所有用户都可以通过这些外部邮箱接收邮件并且自动完成邮件的分发处理，就可以使用此功能。在图 11.8 中选中“ISP 邮件接收”选项卡，打开“ISP 邮件接收”对话框，如图 11.20 所示。

（1）在“ISP 邮件接收转发设定”选项组：在选中“启动经由 ISP 转发邮件的服务”选项后才能设置其他选项。

- 设置更多的 ISP 邮箱下载：为了实现从多个外部 ISP 邮箱中收信，继而按照规则分发给局域网内的所有（或特定）用户，可以使用该功能。单击“更多”按钮，弹出“ISP 设置”对话框，设定需下载的 ISP 邮箱服务器的地址（可以是 IP 地址，如 202.104.32.234；也可以是字符串地址，如 pop.21cn.com），添加到多 ISP 接收列表中。注意：只有加入接收列表的数据才是有效的。
- 设定此 ISP 邮箱的地址（可以是 IP 地址，如 202.106.185.34；也可以是字符串地址，如 pop.21cn.com）。
- 是否启用 ISP 邮件自动分发功能。启用此功能后，下载的 ISP 邮件无论是否有指向，都将会被发送给系统中的所有用户，或者发送给管理员指定的邮件列表用户群。注意：如需发送给邮件列表用户群时，必须要创建相关的邮件列表，并启用邮件列表功能。
- 设定自动分发 ISP 邮件的邮件列表名称。注意：为空时或未启动邮件列表功能时，将分发给系统中所有用户。

（2）在“休眠时间”选项组。

- 设定从 ISP 邮箱中统一接收邮件的间隔分钟数。
- 设定统一进行用户多 POP3 邮件接收的间隔分钟数。

步骤 11：WinWebMail防护

管理邮件系统的安全防护设置。在图 11.8 中选中“防护”选项卡，打开“防护”对话框，如图 11.21 所示。

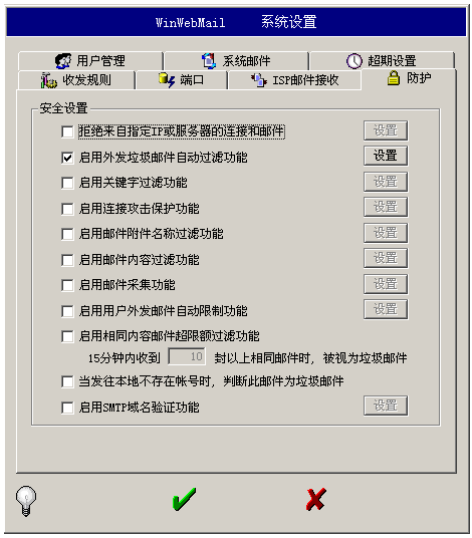

图 11.21　防护管理设置

（1）选中“拒绝来自指定 IP 或服务器的连接和邮件”复选框，单击“设置”按钮，设置系统拒绝服务的 IP 地址或域名。被拒绝后，服务器会直接断开连接，并向连接方显示“554 Unwelcome connection rejected（2）”信息。

（2）选中“启用外发垃圾邮件过滤功能”复选框主要是控制利用邮件服务器向系统外发送垃圾邮件的情况。如果来自同一 IP 地址的每日外发邮件数量过大，系统将会自动封其 IP 地址，并视情况在一段时间后解除。如果是来自被封 IP 地址的连接，服务器会直接断开连接，并向连接方显示“554 Unwelcome connection rejected （4）”信息。

（3）选中“启用关键字过滤功能”复选框，系统将过滤所有主题为指定关键字内容的邮

件。系统将过滤主题等于（不区分大小写）或通配符方式等于指定关键字内容的邮件。这是一个轻量级的过滤功能（占用资源非常少），如果要使用更强大的过滤功能，需要使用邮件内容高级过滤功能。

（4）选中“启用连接保护功能”复选框，主要是用来防御动态连接攻击。如果来自同一 IP 地址的连接数量过大，系统会认为是可疑 IP 地址，并自动限制来自该 IP 地址的连接成功率（如限制接入概率为 20%，即该 IP 地址的每 100 次连接请求中，只允许成功接入 20 次），并视情况在一段时间后解除对此 IP 地址的接入限制。被限制接入后，服务器会直接断开连接，并向连接方显示“554 Unwelcome connection rejected（3）”信息。

（5）选中“启用邮件附件名称过滤功能”复选框，设置系统拒绝接收含有特定附件名称或类型的邮件。

（6）选中“启用邮件内容过滤”复选框，对系统接收到邮件的各项内容进行高级过滤设置。可以针对接收到邮件的各个部分进行细致的过滤功能。

（7）选中“启用邮件采集功能”复选框，将符合条件的邮件采集到指定邮箱中。

（8）选中“启用用户外发邮件自动限制功能”复选框，可以针对用户（而非 IP 地址）进行外发邮件的自动限制。

（9）选中“启用 SMTP 域名验证功能”复选框，单击“设置”按钮，弹出“SMTP 域名验证”对话框，如图 11.22 所示，用来检查 HELO/EHLO 主机名的 A 记录或 MX 记录与连接的 IP 地址是否匹配。（反垃圾邮件效果较好，建议启用）

通常只要设置启用其中的“检查 HELO/EHLO 主机名的 A 记录或 MX 记录”和“检查主机名失败后，检查发送者邮件地址中域名的 A 记录或 MX 记录”两项。更严格的设置是，只启用“检查发送者邮件地址中域名的 A 记录或 MX 记录”功能。

在“未通过检查邮件的处理方式”中建议设置为“拒收”，这样可以避免放入用户垃圾箱后，用户在使用客户端软件时不能及时处理的问题。

步骤 12：WinWebMail事件查看

查看和管理系统事件日志。用鼠标右击 Windows 状态栏上的 WinWebMail 图标，并选择“事件查看”选项，弹出“WinWebMail 事件查看”对话框，如图 11.23 所示。

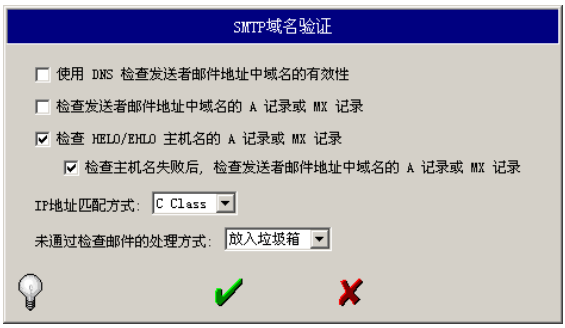

图 11.22 “SMTP 域名验证”对话框

图 11.23 “事件查看”对话框

（1）系统日志文件列表（日志文件位于 \Logs\LogYYYY-MM-DD.txt）。

（2）停止或启动系统日志记录功能。注意：当按钮显示为“停止”时，表示当前系统已经启动了记录功能；而当按钮显示为“启动”时，表示当前系统关闭了记录功能。

（3）启用日志自动删除功能后，系统将只保留指定天数的最近日志数据。

步骤 1 3 ：WinWebMail系统备份

实现系统的自动备份、手动备份及系统恢复功能。用鼠标右击 Windows 状态栏上的 WinWebMail 图标，并选择“系统备份”选项，弹出“WinWebMail 系统备份”对话框，如图 11.24 所示。

（1）系统备份文件列表（备份文件位于 \backup\SysbakYYYY-MM-DD.zip）。

（2）单击“立即备份”按钮，立即将当前系统设置到备份文件“Sysbak.zip”中。

（3）单击“系统恢复”按钮，将当前系统设置恢复为所选中的系统备份文件内容。

（4）选择备份方式，备份的可选方式有 3 种。

- 新式备份：即每次都将当前系统的信息保存到一个指定文件“Sysbak.zip”中。如果该文件已存在，将会被覆盖。
- 量式备份：即为每次备份信息单独创建一个文件保存，其文件名为：SysbakYYYY-MM-DD.zip。
- 备份：不备份当前系统的设置文件。

（5）恢复缺省的系统设置选项。在进行此项操作之前建议先备份好当前系统设置。

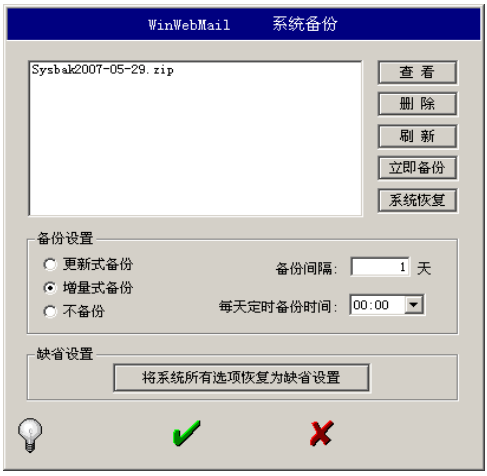

图 11.24 “WinWebMail 系统备份”对话框

步骤 1 4 ：WinWebMail统计信息

对系统中各项功能的用户使用情况进行的数据统计显示。用鼠标右击 Windows 状态栏上的 WinWebMail 图标，并选择“统计信息”选项，弹出“WinWebMail 统计信息”对话框，如图 11.25 所示。

（1）“起始时间”：统计信息显示的起始时间，格式为“YYYYMMDD-HH”。

（2）“显示天数”：图表中显示多少天的数据内容。

（3）“邮件发送”：显示关于邮件发送信息的图表，其中包括：发往本地用户的邮件数量、发往外部（因特网）的邮件数量、通过 WebMail 发送的邮件数量。

（4）“邮件接收”：显示邮件接收信息的图表，其中包括：使用 POP3 下载邮件的数量、多 POP3 下载邮件的数量、ISP 下载邮件的数量。

（5）“WebMail 登录”：显示用户通过 WebMail 登录系统的数量。

（6）“新用户申请”：显示通过 WebMail 申请的新用户数量。

步骤 1 5 ：WinWebMail高级设置

右击 Windows 状态栏上的 WinWebMail 图标，并选择“高级”选项，弹出“WinWebMail 高级”对话框，如图 11.26 所示。

（1）用户页面：进行用户自动清理功能的设置和选项。

（2）邮件页面：设定邮件自动清理的功能和相应选项。

（3）监控页面：监控选定用户的收、发邮件。管理员也可以在 WebMail 界面下设置域邮件监控功能，域邮件监控是针对每个域实现单独监控，即可设置监控任一域内用户所收、发邮件到一个域监控账号中。

（4）Web 页面：对于 WebMail 功能的一些设定。

（5）邮件列表页面：可以实现对部分用户（系统内部）进行邮件群发的功能。

（6）安全页面：启用安全接收控制功能和论及邮件处理功能。

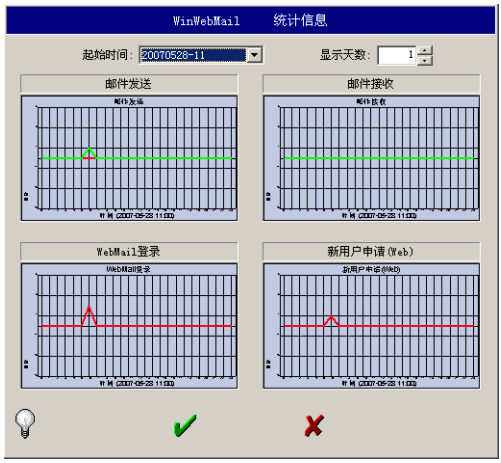

图 11.25 “WinWebMail 统计信息”对话框

图 11.26 “WinWebMail 高级”对话框

习 题

一、名词解释

1．SMTP　　2．POP3　　3．IMAP　　4．MIME

二、填空题

1．电子邮件的格式由信封和内容两大部分，即_____和_____两部分。

2．电子邮件系统使用简单邮件传送协议（SMTP），只能传递_____信息，而通过使用_____，现在还可以发送语音、图像和视频等信息。

3．电子邮件系统由_____、_____和_____ 3 部分组成。

4．在 TCP/IP 互联网中，用户在发送邮件时，要使用邮件发送协议，常见的邮件发送协议有_____ 和_____ 。用户从邮件接收服务器接收邮件时，要使用邮件接收协议，通常使用_____。

5．通常，SMTP 服务器使用 TCP 的_____端口，而 POP3 服务器使用 TCP 的_____端口。

6．电子邮件报文分成两部分：_____和_____，两者之间使用空行分隔。

三、选择题

1．电子邮件的核心是（　　）。

A．电子信箱　　B．邮件服务器

C．邮件地址　　D．邮件客户端软件

2．某用户在域名为 mai.xpc.edu.cn 的邮件服务器上申请了一个电子信箱，邮箱名为 xxzx，那么下面哪

一个是为该用户的电子邮件地址？（　　）

A．mail.xpc.edu.cn@xxzx　　B．xxzx%xpc.edu.cn

C．mail.xpc.edu.cn%xxzx　　D．xxzx@mail.xpc.edu.cn

四、思考题

1．电子邮件的格式是怎样构成的？请举例说明。

2．电子邮件系统由哪几部分组成？

3．简述电子邮件的发送和接收过程。

4．如何在电子邮件中夹带其他形式的文档？

5．SMTP 的作用是什么？

6．POP3 的作用是什么？

7．IMAP 的作用是什么？

五、实训题

1．在网易中申请免费电子信箱。

2．学会使用 Web 方式的信箱进行邮件的发送、接收并添加附件等操作。

3．在 Outlook 中如何设置在网易中申请的信箱。

项目 12　安装和配置终端服务

12.1　项目内容

1．项目目的

在了解终端服务的基础上，掌握在 Windows Server 2003 操作系统中配置终端服务器，并熟悉终端服务客户端的使用方法。

2．　项目任务

在单位局域网内部，网络管理员希望在任何一台计算机上都能管理网络中的服务器，同时网络中还存在一些低配置的客户端，用户希望在这些计算机上也能运行一些对硬件要求高的程序。

3．任务目标

① 掌握终端服务器的安装；
② 掌握终端服务客户端的使用方法；
③ 掌握终端服务器远程管理方法。

12.2　相关知识

12.2.1　终端服务概念

终端服务（Terminal Services）是一个客户端/服务器应用程序，服务器端只能是 Windows Server 2003 家族系统，而客户端不做限制，但需要安装有终端服务客户端软件。

终端服务客户端是一个小型终端仿真程序，它只提供到服务器上运行的软件的接口。用户通过客户端连接软件来连接终端服务器时，必须输入用户名和密码来登录，之后他的屏幕上所显示的就是 Windows Server 2003 的桌面，然后就可以执行终端服务器内的应用程序、存储文件、使用网络资源，就好像他是在使用这台远程服务器一样。

这些应用程序是在终端服务器（而不是在用户的计算机）内执行的，用户只在他的计算机上通过键盘与鼠标来操作应用程序，然后将终端服务器所传送来的结果显示在屏幕上。

通过终端服务，几乎可以从网络上的任何计算机对计算机进行管理。可使用管理远程桌面来远程登录到服务器，就好像从本地登录一样。远程管理桌面基于终端服务技术，是为管理服务器上的远程桌面连接而专门设计的。

12.2.2　终端服务功能

Windows Server 2003 终端服务器可用来管理每个客户远程登录的资源，它提供了一个基于远程桌面协议（RDP）的服务，使 Windows Server 2003 成为真正的多会话环境操作系统，并让用户能使用服务器上的各种合法资源。

Windows Server 2003 通过终端服务的技术，具有提供以下功能。

1．远程桌面管理

可以让系统管理员远程管理网络与计算机，内含在 Windows Server 2003 系统内，不需要另外安装，不过每一台计算机最多只允许 2 位系统管理员来连接（即以前版本终端服务器中的“远程管理模式”）。

2．多人同时执行位于终端服务器内的应用程序

在 Windows Server 2003 系统内安装了终端服务器的组件后，就可以在这台终端服务器内安装应用程序，这个应用程序可以让网络上的多个用户同时执行，而且这些用户的计算机可以是 Windows Server 2003、Windows XP、Windows 2000、Windows NT、Window9×等系统的。

12.2.3 终端服务的组成

终端服务主要由以下 3 个组件组成：

1．终端服务器

终端服务器是指运行终端服务的 Windows Server 2003 计算机，该服务器允许客户端连接到服务器上，并运行服务器内的应用程序，同时将服务器处理的结果送还到客户机上，显示在客户机的屏幕上。

2．客户机

客户机是指安装终端服务客户端软件的计算机，客户机利用客户端软件连接到服务器上，并向服务器发送数据，调用服务器上的运算资源为其运行应用程序或执行远程管理。

客户端可以是计算机、基于 Windows 的终端设备和其他设备（如 Mac 计算机或基于 UNIX 的工作站等），这些设备也可以使用第三方的远程软件连接到终端服务器。

3．远程桌面协议

远程桌面协议（Remote Desktop Protocol，RDP）是一个基于 ITU（International Telecommunication Union）T.120 标准的通信协议，该协议依赖 TCP/IP 协议的多信道通信协议。RDP 用于负责客户端与服务器之间的通信，传输显示在客户端的图形数据，使客户端的用户看起来好像坐在服务器前亲自操作服务器一样。

12.3 方案设计及准备

1．设计

架设一台基于 Windows Server 2003 的终端服务器。根据要求，本项目实施的网络拓扑图如图 12.1 所示。

图 12.1 终端服务网络拓扑图

2．设备清单

为了搭建图 12.1 所示的网络环境，需要下列设备：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 安装 Windows XP 的计算机 1 台。

12.4 项目实施

“远程桌面连接”远程管理模式是网络管理员在服务器或客户机上通过网络对远程计算机或服务器进行管理的一种方式，属于 C/S 模式。

步骤 1：终端服务器的安装

在扮演终端服务器角色的 Windows Server 2003 计算机（如设置 IP 地址为 192.168.11.243）上执行以下操作步骤来完成终端服务器的安装。

（1）选择“开始→设置→控制面板→添加或删除程序”命令，进入“添加/删除程序”对话框，单击“添加/删除 Windows 组件”按钮，弹出“Windows 组件向导”对话框，在“组件”列表框中勾选“终端服务器”、“终端服务器授权”复选项，如图 12.2 所示。

（2）单击“下一步”按钮，系统会弹出一个提示框，单击“是”即可随后显示终端服务的介绍窗口，包括有关配置远程访问和 120 天授权的内容，如图 12.3 所示。

（3）单击“下一步”按钮，弹出“终端服务器安装程序的安全模式”对话框，如图 12.4 所示。终端服务器安全模式有两种：完整安全模式和宽松安全模式。一般情况下，选择完整安全模式。

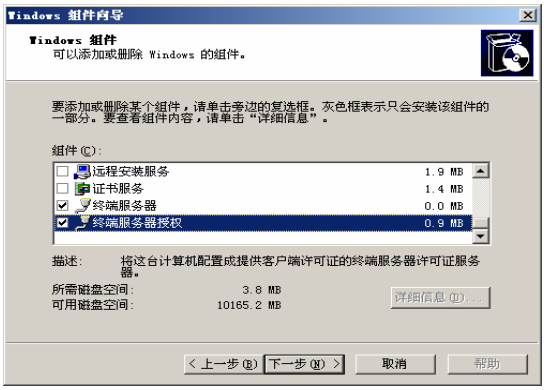

图 12.2 “Windows 组件”对话框

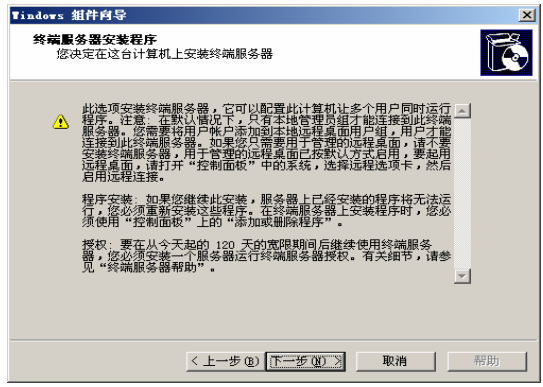

图 12.3 “终端服务器安装程序”对话框

（4）单击“下一步”按钮，弹出“终端服务器安装程序”的选择许可证服务器对话框，如图 12.5 所示，选择“我将在 120 天内指定许可证服务器”单选按钮。

（5）单击“下一步”按钮，弹出“授权模式”对话框，如图 12.6 所示，选择“每设备授权模式”单选按钮。

（6）单击“下一步”按钮，弹出“数据库文件位置”对话框，如图 12.7 所示，默认设置，单击“下一步”按钮，完成配置，单击“完成”按钮，完成终端服务器的安装。重新启动计算机。

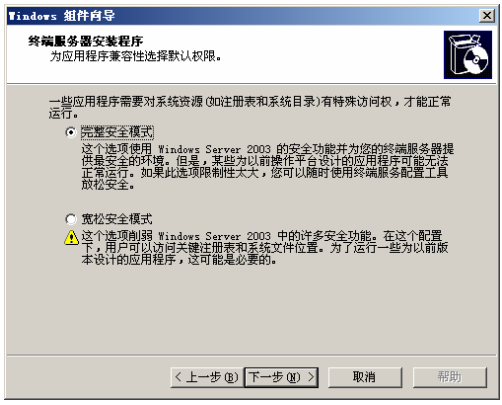

图 12.4 “安全模式”对话框

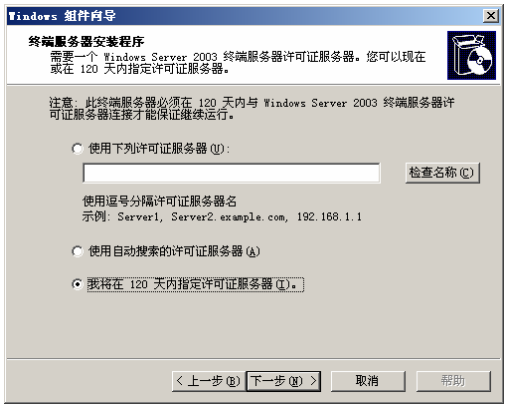

图 12.5 “选择许可证服务器”对话框

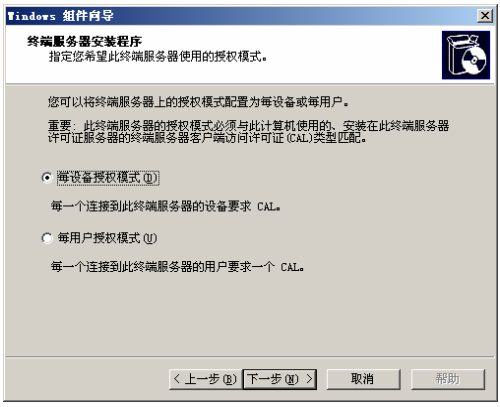

图 12.6 “授权模式”对话框

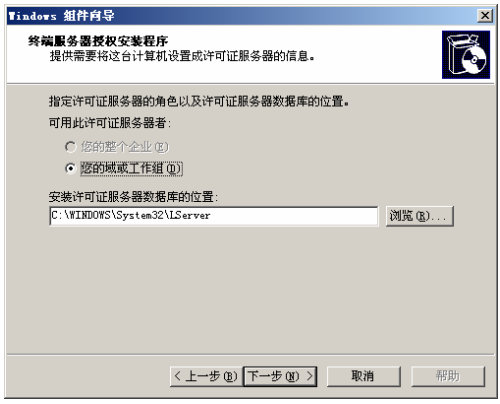

图 12.7 “数据库文件位置”对话框

步骤 2：终端服务器授权

终端服务器安装后，只有 120 天的使用期限，这时需要在网络内有一台已经被激活的“终端服务器授权服务器（Terminal Server License Server）”，并且取得合法的授权连接数量。

终端服务器授权过程如下：

（1）按照步骤 1 完成终端服务器的安装。

（2）选择“开始→程序→管理工具→终端服务器授权”命令，打开“终端服务器授权”窗口，其中有一个没有激活的终端服务器。

（3）右击要激活的授权终端服务器，在弹出的菜单中选择“激活服务器”选项，启动授权向导，单击“下一步”按钮。弹出“连接方法”对话框，选择注册的连接方法，如图 12.8 所示。

（4）单击“下一步”按钮，弹出“公司信息”对话框，添加各栏目信息，单击“下一步”按钮，弹出“公司信息（可选）”对话框，添加各栏目信息。

（5）单击“下一步”按钮，进行激活，按照向导完成终端服务器授权。

图 12.8　终端服务器授权

步骤 3：配置远程访问

1）启动远程桌面

必须在提供终端服务的计算机上启动“远程桌面”的功能，并且在将用户账户加入到 Remote Desktop Users 组后，用户才可以利用“远程桌面连接”来连接终端服务器或远程计算机。

- 如果未安装终端服务器，只提供远程桌面管理的功能，则依次选择“开始→设置→控制面板→系统”，打开“系统属性”对话框，选择“远程”标签，选中“启用这台计算机上的远程桌面”复选框来启动远程连接的功能。如图 12.9 所示。然后单击“选择远程用户”按钮，单击“添加”按钮将用户加入到 Remote Desktop Users 组。
- 如果是域控制器，则选择“Active Directory 用户及计算机”将用户加入到 Remote Desktop Users 组内，这个组位于 builtin 区之内。
- 如果是成员服务器或独立服务器，则依次选择“开始→程序→管理工具→计算机管理→系统工具→本地用户和组”，将用户加入到 Remote Desktop Users 组。

同时 Remote Desktop Users 还必须具备“允许通过终端服务登录”的权限。在 Windows Server 2003 成员服务器、独立服务器与 Windows XP 计算机内，Remote Desktop Users 默认已经具备了这个权限。但在域控制器上，Remote Desktop Users 组没有这个权限，因此必须另外赋予权限后，用户才可以远程连接。开放此权限的途径为：到域控制器上依次选择“开始→程序→管理工具→域控制器安全策略→安全设置→本地策略→用户权限分配”，弹出“本地安全设置”对话框，如图 12.10 所示，双击右侧窗口的“通过终端服务允许登录”，添加 Remote Desktop Users 组。

2）增加远程访问用户

（1）选择“开始→管理工具→计算机管理”命令，弹出“计算机管理”窗口。

（2）依次展开“系统工具”、“本地用户和组”、“组”。

（3）从“组”右边的列表框中选择“Remote Desktop Users”，鼠标右击并选择“属性”选项，弹出“Remote Desktop Users 属性”对话框，单击“添加”按钮，弹出“选择用户”对话框，如图 12.11 所示。

（4）单击“高级”按钮，单击“立即查找”按钮，从“搜索结果”列表框中选择用户，

两次单击“确定”按钮，单击“应用”按钮，单击“确定”按钮，退出“计算机管理”窗口。

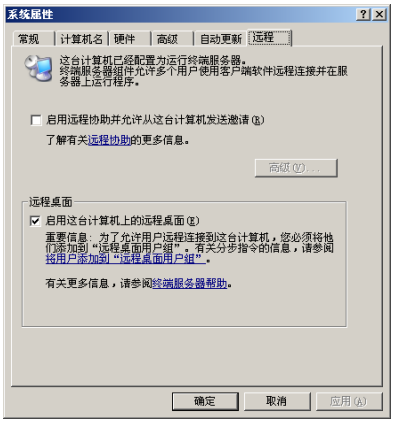

图 12.9　“远程”标签

图 12.10　“本地安全设置”窗口

图 12.11　远程访问用户管理

步骤 4：配置终端服务器

选择“开始→管理工具→终端服务设置”命令，打开“终端服务配置”对话框，如图 12.12 所示。在终端服务器配置目录树下有两种配置：连接和服务器设置。

1）终端服务的连接配置

在“终端服务配置”对话框中单击“连接”，在右边窗口中选中 RDP-Tcp 的默认连接，右击，在弹出的菜单中选择“属性”选项，弹出“RDP-Tcp 属性”对话框，如图 12.13 所示。

RDP-Tcp 连接是客户端连接服务器上进行远程桌面管理与终端服务器共享应用程序所需要配置的唯一连接。只能为每个网络适配器配置一个 RDP 连接，如果要配置其他的 RDP 连接，必须安装其他网络适配器。

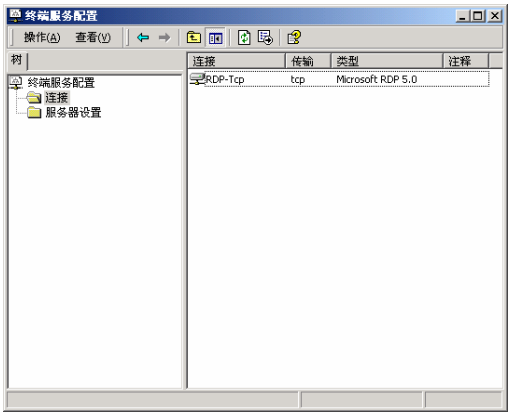

图 12.12 “终端服务配置”窗口

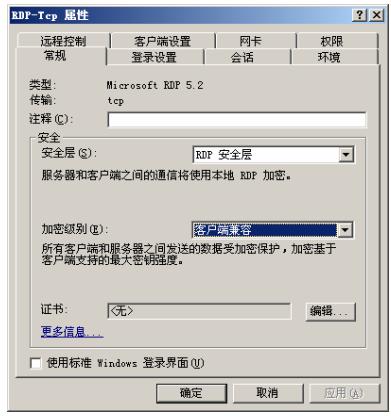

图 12.13 常规设置

（1）“常规”选项卡。“RDP-Tcp 属性” 对话框的“常规”选项卡主要用于设置对客户机和终端服务器之间的通信进行加密保护的级别，共有 4 种加密级别。

- 高级：该加密级别使用 128 位的强加密算法来加密客户机和服务器之间的数据。只有当终端服务器运行在仅包含 128 位客户机的环境下（例如远程桌面连接客户机）时才使用该级别。不支持该级别加密的客户机将不能连接。
- 客户机兼容：该加密级别以客户机所能支持的最大密钥强度来加密在客户机和服务器之间传送的数据。当终端服务器运行在混合环境或者包含旧有客户机的环境中时，应该使用该级别。
- 低级：该加密级别使用 56 位的加密算法来加密从客户机发往服务器的数据，但从服务器发往客户机的数据不进行加密。
- 符合 FIPS 标准：该加密级别使用 Microsoft 加密模块，通过联邦信息处理标准（FIPS）加密算法，对客户端和服务器之间传送的数据进行加密和解密。如果“符合 FIPS 标准”已经由组策略“系统加密：对加密，散列和签名使用符合 FIPS 算法”所启用，管理员便不能通过更改终端服务“设置客户端连接加密级别”组策略设置或通过终端服务配置来更改终端服务连接的加密级别。

（2）“登录设置”选项卡。“RDP-Tcp 属性” 对话框的“登录设置”选项卡主要用于设置客户机能够登录终端服务器的用户名和口令。如图 12.14 所示。

要使用自动登录，需选中“总是使用下列登录信息”单选按钮，在“用户名”文本框中输入允许自动登录到服务器的用户的名称，在“密码”和“确认密码”框中输入该用户的密码。这样客户端连接时将不用再输入用户名和密码，而自动进入 Windows Server 2003 桌面（注意：若此后再有用户登录，那么原来的连接将被断开）。若输入不完整，则登录时还会要求输入用户名或密码。

如要想更安全地使用服务器，则应选中“总是提示密码”复选框以指定该用户在登录到服务器之前始终要被提示输入密码，从而限制客户端的自动登录。

（3）“会话”选项卡。“RDP-Tcp 属性”对话框的“会话”选项卡主要用于设置活动的、断开连接的以及空闲的会话在服务器上保留的时间，以便释放会话所占用的资源，如图 12.15 所示。

“结束已断开的会话”和“空闲会话限制”的时间，一般设为 5 分钟较好。对安全性要求高的也可设定“活动会话限制”的时间。“达到会话限制或者连接被中断时”下的选项，最好选择“结束会话”选项，这样连接所占的资源就会被释放。

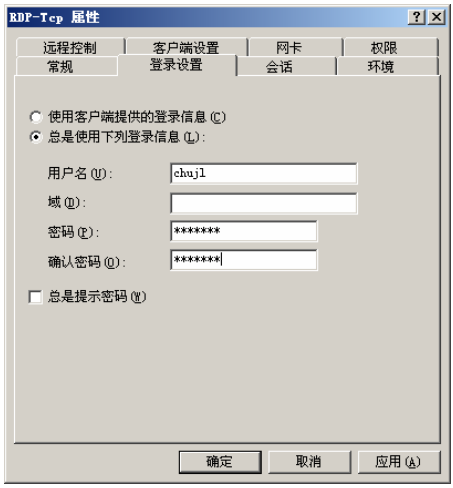

图 12.14　登录设置

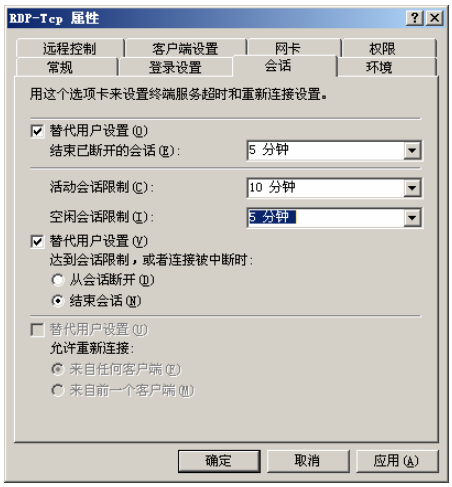

图 12.15　会话设置

（4）“环境”选项卡。“RDP-Tcp 属性”对话框的“环境”选项卡主要用于设置客户机登录后启动的服务器上的初始程序，如图 12.16 所示。

如果在“初始程序”选项组中选择“运行用户配置文件指定的初始程序和远程桌面连接或终端服务客户端的设置”单选按钮，则当用户登录的时候自动启动的应用程序由下面的“程序路径和文件名”框中的设定来决定。如果不选择该单选按钮，则用户在“用户配置文件”或在“客户端连接管理向导”中设定的应用程序会启用。

（5）“远程控制”选项卡。“RDP-Tcp 属性”对话框的“远程控制”选项卡如图 12.17 所示，可以进行如下设置：

① 使用具有默认用户设置的远程控制：表示用户是否可被远程控制，是通过用户账号的属性来设置的。可以利用“本地用户和组”来检查和设置。

② 不允许远程控制：终端服务器不允许任何人映射其他计算机与服务器的会话到自己，不允许控制其他客户端与服务器之间的操作。

③ 使用具有下列设置的远程控制：设置所有的用户都可被远程控制，并且利用以下的设置决定如何来远程控制。

- 需要用户权限：当开始要远程控制时，是否要在客户端的屏幕上显示信息，并经客户端同意后才可以远程控制。
- 查看会话：只能够监视客户端与终端服务器之间的运行，无法利用键盘或鼠标来控制。
- 与会话交互：可以利用鼠标或键盘操作、控制客户端与服务器之间的会话中所有的运行。

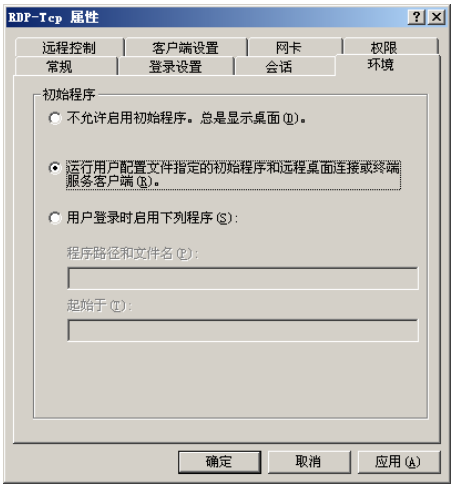

图 12.16　环境设置

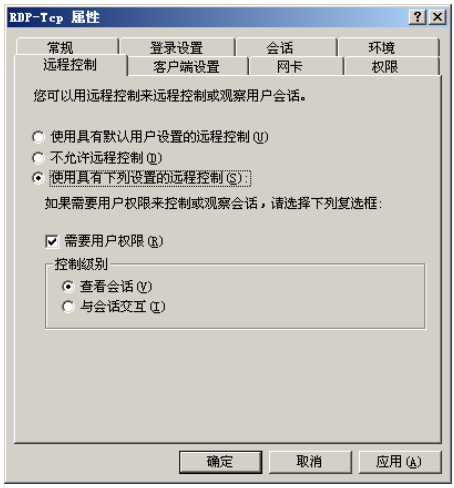

图 12.17　远程控制设置

（6）“客户端设置”选项卡。“RDP-Tcp 属性”对话框的“客户端设置”选项卡对话框如图 12.18 所示，可以设置的参数有以下这些。

① “连接”选项组中：

- 选择“登录时连接客户端驱动器”复选框，将在登录时重新连接所有映射的客户端驱动器，该选项卡仅支持运行任何 Windows Server 2003 操作系统的客户端。
- 选择“登录时连接客户端打印机”复选框，将在登录时重新连接所有映射的本地客户端打印机。
- 选择“将默认值设为主客户端打印机”复选框，将打印作业发送到客户端的默认打印机，否则服务器的默认打印机将作为所有客户端会话的默认打印机使用。

② 选择“颜色深度最大值”复选框，在下拉列表框中选择要限制客户端使用的颜色深度最大值。限制颜色深度可以增强连接性能，尤其是对于慢速连接，并且还可以减轻服务器负载。“远程桌面”连接的当前默认最大颜色深度设置为 16 位。

选中“颜色深度最大值”，可修改限定的最大颜色深度为 8、15、16 或 24 位。若不选中，则使用登录的客户端颜色设置。

③ “禁用下列项目”选项组中：

- 选择“驱动器映射”复选框，禁止客户端使用驱动器映射功能。
- 选择“LPT 端口映射”复选框，禁止客户端手动创建 LPT 端口的打印机。
- 选择“Windows 打印机映射”复选框，禁止客户端使用 Windows 打印机映射功能。
- 选择“COM 端口映射”复选框，禁止客户端使用 COM 端口映射功能，无法手动创建使用 COM 端口的打印机。
- 选择“剪贴板映射”复选框，禁止客户进行剪贴板映射。
- 选择“音频映射”复选框，禁止客户端使用音频映射功能。

（7）“网卡”选项卡。“RDP-Tcp 属性”对话框的“网卡”选项卡用于设置网络上的网卡上可以接受的同时连接的会话数，如图 12.19 所示。

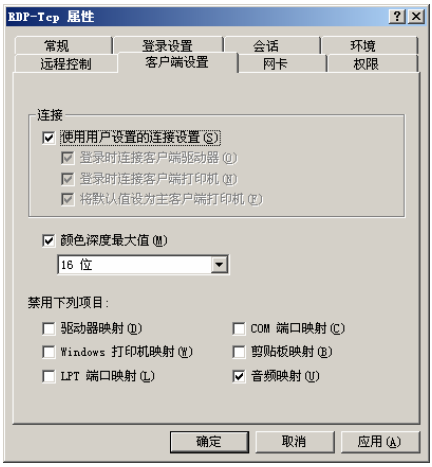

图 12.18　客户端设置

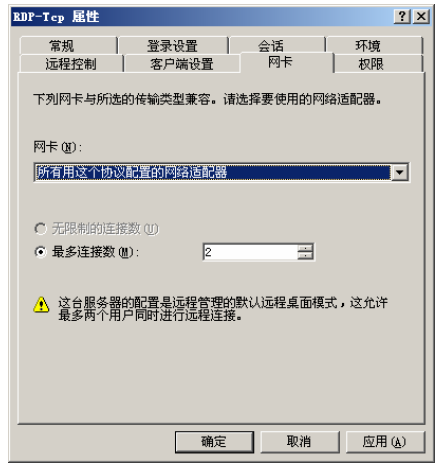

图 12.19　网卡设置

设置更多的连接数可使更多的用户同时登录服务器。默认最多同时 2 个用户连接，如果想要使 3 个以上的用户同时使用远程桌面功能，则必须安装终端服务，安装后就可以任意设定用户数。

由于每个用户连接远程桌面后最小占用 12MB 左右的内存，因此可根据服务器内存大小来设定用户数，一般用户数不要太多，以免影响性能。如 256MB 内存可设定用户数 8 个左右，512MB 内存可设定 20～30 个。

（8）“权限”选项卡。“RDP-Tcp 属性”对话框的“权限”选项卡用于设置远程登录的用户和组如何访问终端服务器。通过权限进行控制，可以确保服务器的安全，如图 12.20 所示。

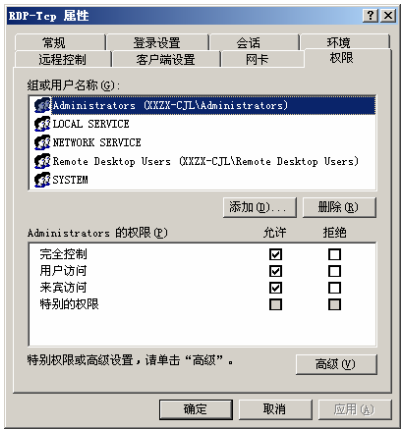

图 12.20　权限设置

① 远程客户机访问服务器的权限有 4 种。

- 完全控制：允许用户查询有关会话的信息、修改连接参数、复位会话、远程控制另一用户的会话、登录到服务器上的会话、从会话中注销用户、向另一个用户会话发送消息、连接到其他会话、断开会话、使用虚拟通道提供从服务器程序访问客户端设备的能力。
- 用户访问：允许用户登录到服务器上的会话、查询有关会话的信息、向其他用户会话

发送消息和连接到其他会话。

- 来宾访问：允许用户登录到服务器上的会话。
- 特别的权限：允许用户查询有关会话的信息，向另一会话发送消息。

② “高级”权限设置。

单击“高级”按钮，打开“RDP-Tcp 的高级安全设置”对话框，如图 12.21 所示。在“权限”选项卡中，选择需要更改权限的用户或组，然后单击“编辑”按钮，打开“RDP-Tcp 的权限项目”对话框。如图 12.22 所示。在“权限”中，根据需要在要为该组设置的权限旁选中或清除“允许”或“拒绝”复选框。

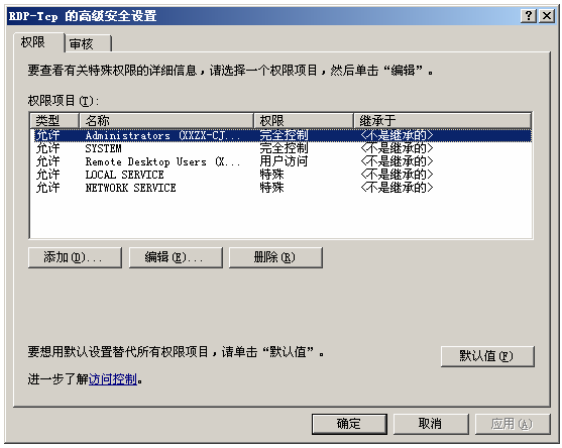

图 12.21　高级安全设置

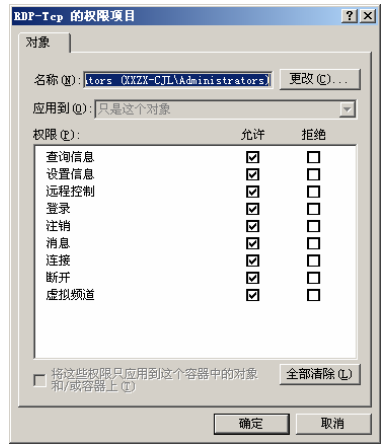

图 12.22　权限项目设置

2）终端服务器设置

在“终端服务配置”对话框中（图 12.12），选择“终端服务器配置”下的“服务器设置”选项，如图 12.23 所示。

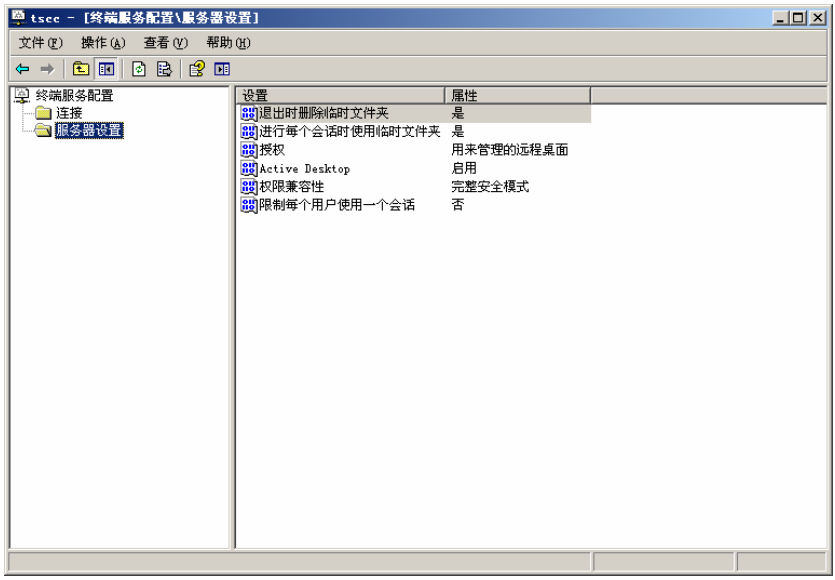

图 12.23　“终端服务配置－服务器设置”对话框

（1）退出时删除临时文件夹：默认情况下，终端服务器会为服务器上的每个新会话创建单独的临时文件夹，使每个用户都可以存储各自的临时文件。双击该选项，选择“是”表示当用户从会话中注销时会删除这些临时文件夹。

（2）进行每个会话时使用临时文件夹：双击该选项，选择“是”表示设置多用户使用不同临时文件夹，选“否”为相同，同样可设置退出时是否删除临时文件夹。

（3）授权：双击该选项，在弹出的“授权模式”对话框中，选择“每设备”或“每客户”授权许可模式。

（4）Active Desktop：该选项用于设置是否允许客户端运行服务器的 Active Desktop（活动桌面）功能，为节省系统资源，默认情况下该功能被禁用。

（5）权限兼容性：该选项用于设置通过远程运行的应用程序的处理模式。双击该选项，可以选择“完整完全模式”和“宽松安全模式”。

- 完整完全模式：该模式下终端服务器用户与服务器上的用户组的成员相同的权限。这是最安全的模式，但有些应用程序在该模式下无法运行。
- 宽松安全模式：该模式下所有用户将拥有对关键的注册表和文件系统位置的完全访问权。如果要在终端服务的客户机上运行有些老的应用程序，则需要选择此模式。

（6）限制每个用户使用一个会话：双击该选项，选择“是”为限制一个用户登录，去掉其中的选项(即选“否”)允许多用户同时自动登录，可使多个用户以相同用户名连接到相同的服务器，使得一般的多用户应用非常方便。

步骤 5：远程桌面程序的安装

假设在一台 IP 地址为 192.168.11.22 的计算机上安装终端服务客户端。

客户端若要连接到终端服务器，则这些计算机内必须安装“远程桌面连接（Remote Desktop Connection）”软件。Windows Server 2003 和 Windows XP 已经内含“远程桌面连接”，不需要再安装。

Windows 2000/NT/ME/9×等客户端必须要另外安装“远程桌面连接”软件。

远程桌面连接安装文件位于终端服务器内（Windows Server 2003 系统）的%systemroot% system32\clients\tsclient\win32 文件夹内。

将该文件夹内的 5 个文件复制到客户机上，双击 setup.exe 文件就可以在客户机上执行远程桌面程序的安装。安装过程比较简单，在这里不再详述。

步骤 6：连接终端服务器

下面用一台 Windows XP 计算机（192.168.11.22）利用“远程桌面连接”来连接终端服务器（IP 地址为 192.168.11.243）。

（1）选择“开始→程序→附件→通讯→远程桌面连接”命令，弹出“远程桌面连接”对话框，如图 12.24 所示。在“计算机”下拉列表框中可以选择或输入终端服务器的 IP 地址、计算机名称或 DNS 主机名称。

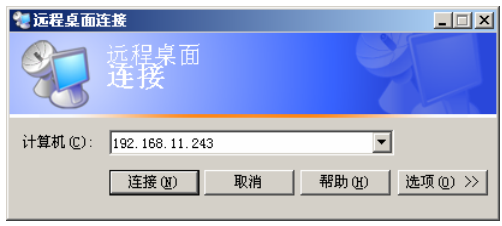

图 12.24　远程桌面连接

图 12.25　输入用户名和密码

（2）单击“连接”按钮，弹出“远程桌面”对话框，输入用户登录的用户名和密码，如图 12.25 所示。输入用户名和密码，单击“确定”按钮后出现和远程服务器上完全一致的界面，然后就可以执行远程管理了。

（3）登录以后，在客户机的桌面上将出现一个浮动工具栏，单击工具栏右侧的关闭按钮将出现提示界面，此操作将断开同 Windows 会话的连接，单击“确定”按钮将关闭远程桌面连接。

可以按 Ctrl＋Alt＋Break 组合键将其切换到全屏模式。在实际操作时，画面中间最上方会有一条黄色的区域，上面显示终端服务器的 IP 地址或计算机名称。

（4）如果出现终端服务器如图 12.26 所示的“中断远程桌面连接”对话框，则可能的原因是：终端服务器拒绝该客户机的连接、计算机太忙或者系统资源不够、服务器没有启动远程桌面连接功能。

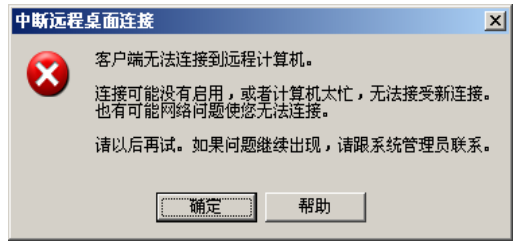

图 12.26　中断远程桌面连接

对于前两种原因，客户端可以与服务器管理员联系排除故障。

对于第 3 个原因是终端服务器的远程连接功能没有启用。

（5）注销或中断连接。用户要结束与终端服务器的连接时，可以通过以下方法：

- 注销：用户注销后，其在终端服务器上所执行的程序会被结束。依次单击远程桌面窗口内左下角的“开始→注销”，或是按 Ctrl＋Alt＋End 组合键，当弹出“Windows 安全性”画面时，单击“注销”按钮。
- 中断：中断连接并不会结束用户正在终端服务器上执行的程序，这些程序仍然会在终端服务器上继续执行，而且桌面环境也会被保留。

步骤 7：远程桌面连接的高级设置

单击“选项”按钮，弹出“远程桌面连接”对话框，进行远程桌面连接的高级设置。

（1）“常规”选项卡。在图 12.27 中，在“登录设置”选项组设置终端服务器的 IP 地址或域名、登录的用户名、密码和所在计算机域。

在“连接设置”选项组用于保存或打开连接参数的设置。

（2）“显示”选项卡。选择“显示”选项卡，如图 12.28 所示，用于设置如何显示远程服务器的桌面，包括远程桌面的大小和颜色等。

（3）“本地资源”选项卡。选择“本地资源”选项卡，用于设置远程计算机声音是否在客户机上播放，是否使用本地键盘和是否启用客户机本地的磁盘驱动器、打印机和串行口等。

（4）“程序”选项卡。选择“程序”选项卡，可以设置用户在登录终端服务器后首先运行的远程服务器的程序。

（5）“高级”选项卡。选择“高级”选项卡，用于设置是否允许桌面更换背景、拖拉时是否显示窗口内容、是否显示菜单和窗口动画、是否启用主题和是否启用位图缓存等功能。

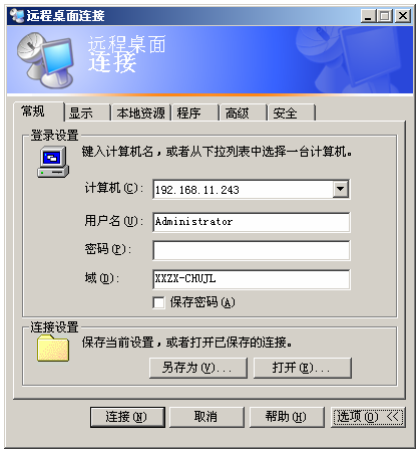

图 12.27　常规设置

图 12.28　显示设置

步骤 8：利用终端服务管理器管理终端连接

利用终端服务管理器，可以监视和控制连接到网络上的所有终端服务器的连接。在“终端服务管理器”窗口中，不仅可以看到网络上有哪些有效的终端服务器，还能够看到有谁连接到它们、正在执行哪些工作任务，以及使用了哪些协议等。

终端服务管理器的使用方法如下。

（1）选择“开始→程序→管理工具→终端服务管理器”命令，弹出“终端服务管理器”对话框，展开“这台计算机”及其子项。

其中节点“RDP –Tcp#2（administrator）”是远程访问的连接。

（2）选中“RDP –Tcp#2（administrator）”选项，右击并从菜单中选择“发送消息”选项，弹出“发送消息”对话框，输入发送信息，如“请及时退出，10 分钟后关闭服务器”，如图 12.29 所示。单击“确定”按钮，将消息发送到客户端。

（3）选中“RDP –Tcp#2（administrator）”选项，右击并从菜单中选择“断开”选项，可以强行中止客户端的远程连接。

步骤 9：在终端服务器上安装应用程序

在安装应用程序前，必须将终端服务器切换到“安装模式”，完成安装后，必须再将其切换回“执行模式”。安装应用程序的方法有以下两种：

（1）利用“控制面板”内的“添加/删除程序”：安装应用程序时，系统自动切换到“安装模式”，完成安装后，必须再将其切换回“执行模式”。

（2）配合 change user 命令，使用其他方法安装应用程序：如执行 setup.exe，则必须手动执行 change user /install 命令将系统切换到“安装模式”，完成安装后，再执行 change user /execute 命令将系统切换到“执行模式”。

使用 change user /query 命令，查看终端服务器目前是处于“安装模式”还是“执行模式”。

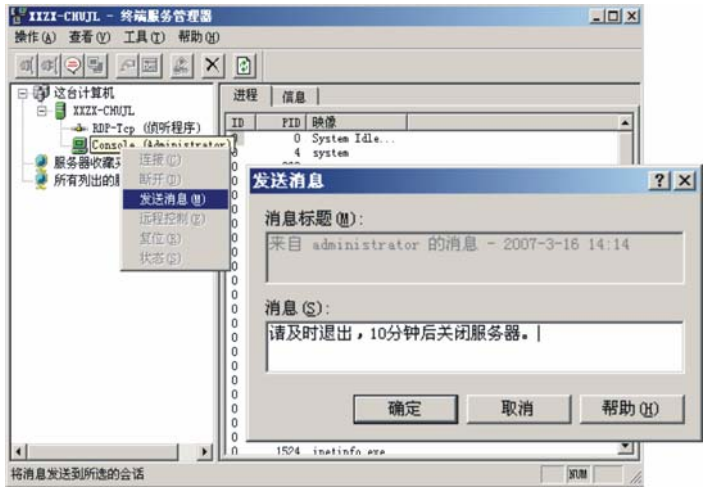

图 12.29　设置本地域名服务器

习　题

一、填空题

1．终端服务主要由_____、_____和_____3 个组件组成。

2．远程桌面连接是网络管理员在服务器或客户机上通过网络对_____进行管理的一种方式。

3．远程桌面管理工具使用_____协议在服务器和客户端间建立连接。

4．远程桌面管理使用_____和_____两个工具实现远程管理。

二、选择题

1．在下列网络服务中，（　　）是远程登录服务，默认端口号为（　　）。

（1）A．WWW　　B．FTP　　C．BBS　　D．Telnet

（2）A．21　　B．23　　C．25　　D．80

2．Telnet 提供的服务是（　　）。

A．远程登录　　B．电子邮件

C．域名解析　　D．寻找路由

三、思考题

1．什么是终端服务？

2．终端服务的功能有哪些？

3．终端服务的组成是什么？

四、实训题

1．配置一台远程管理服务器，实现管理员可以在网络的任何一点远程管理该服务器；

2．配置一台终端服务器，新建一个 wluser 用户,使其具有访问终端服务权限，并以该用户身份登录终端服务器；管理员可以监控远程用户访问终端服务器。

项目 13　使用WSUS升级操作系统补丁

WSUS（Windows Server Update Service）是 SUS 的升级版本，是微软公司推出的用于局域网内计算机操作系统升级的一种服务器软件，它可以快速、方便地为网络中的每台工作站升级操作系统补丁。

13.1　项目内容

1．项目目的

在了解 WSUS 工作原理的基础上，掌握在 Windows Server 2003 系统中配置 Update 服务器的方法，并熟悉终端用户策略的配置方法。

2．项目任务

在单位局域网内部，网络管理员希望在单位内部架设一台 Update 服务器系统，使局域网内的计算机用户都能够及时到 Update 服务器上更新操作系统的补丁，增强计算机用户终端的安全性。

3．任务目标

① 掌握 WSUS 的安装；
② 掌握 WSUS 的配置；
③ 掌握用户终端计算机策略的配置。

13.2　相关知识

使用 Windows 自带的 Update 下载补丁，速度比较慢，可以利用微软提供的 WSUS 建立一个内部 Update 服务器，让公司内网中的计算机直接到这台 Update 服务器上下载补丁，以缩短用户打补丁的时间，及时提高计算机和网络的安全性。

13.2.1　WSUS特点

WSUS 与 SUS 相比，具有以下的特性：

- 支持对更多微软产品进行更新，如 Office、Exchange、SQL 等产品的补丁和更新包都可通过 WSUS 发布，而 SUS 只支持 Windows 系统。
- 提供了中文操作界面，以前的 SUS 操作界面为英文，不便于操作。
- 通过 BITS2.0（Background Intelligent Transfer Service）来最大化有效带宽，比 SUS 更好地利用了网络带宽。
- 对客户机的管理更强大，可针对不同客户机分配不同的用户组，并分配不同的下载规则。

➢ 在设置和管理上比 SUS 更简单直观。

13.2.2 使用WSUS的注意事项

在安装 WSUS 之前，先完成以下工作：

（1）WSUS 不能在安装了“终端服务”的计算机上进行安装，应该先安装 WSUS，然后再安装终端服务进行远程管理。

（2）在安装 WSUS 之前，需要安装 Microsoft.net、Framework 1.1、Service Pack1 和 BITS2.0。

（3）如果在安装 WSUS 之后，WSUS 不能运行或出现错误，则需要修改 C:\windows\Microsoft.NET 和 C:\windows\temp 文件夹的安全性。在 Windows Server 2003 系统上，需要添加“Network Service 账户”对这两个文件夹的读写权。

（4）WSUS 必须要有 IIS 的支持。

（5）在安装 WSUS 之后，在管理员工作站上，最好使用 Microsoft 的 IE 浏览器进行管理，并且必须将 IE 配置为允许活动脚本。

13.3 方案设计及准备

1．设计

在单位内部局域网中一台安装 Windows Server 2003 的计算机上利用微软提供的 WSUS（Windows Server Update Services）建立一个内部 Update 服务器，让公司内网中的计算机直接到这台 Update 服务器上下载补丁。架设一台基于 Windows Server 2003 的终端服务器。根据要求，本项目实施的网络拓扑图如图 13.1 所示。

图 13.1 WSUS 网络拓扑图

2．设备清单

为了搭建图 13.1 所示的网络环境，需要下列设备：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 安装 Windows XP 的计算机 1 台。

13.4 项目实施

步骤 1：WSUS的安装

安装 WSUS 的系统分区需要 1GB 磁盘空间，存储数据库文件的卷需要 2GB，WSUS 的补丁估计需要 6GB。首先到微软网站下载 WSUS 文件，下载地址为 http://download. microsoft. com /download/9/3/3/933eaf5d-f2a2-4a03-8a87-e8f6e6d07e7f/ WSUSSetup.exe。

（1）运行下载的 WSUS 安装程序包（文件名为 WSUSSetup.exe，大小为 124MB），进入

WSUS 的安装界面，单击“下一步”按钮，弹出“许可协议”对话框，选择“我接受许可协议中的条款”单选按钮，单击“下一步”按钮，弹出“选择更新源”对话框。通常情况下，安装程序会选择可用空间最大的磁盘分区，根据需要进行选择，如图 13.2 所示。

（2）单击“下一步”按钮，弹出“数据库选项”对话框，选择数据库保存路径，如图 13.3 所示。在 Windows Server 2003 系统上，WSUS 安装自带的 MSDE 数据库，通过其数据库保存磁盘至少要有 2GB 可用空间。如果数据库与 WSUS 下载的补丁在同一分区，则至少需要 8GB 的可用空间。

图 13.2 “选择更新源”对话框

图 13.3 “数据库选项”对话框

（3）单击“下一步”按钮，弹出“网站选择”对话框，选择 WSUS 管理工具和服务网站使用的端口号。如图 13.4 所示。如果是全新安装的 WSUS，可以选择使用 TCP 的 80 端口或 TCP 的 8530 端口；如果是升级安装，只能选择 TCP 的 8530 端口。

图 13.4 “网站选项”对话框

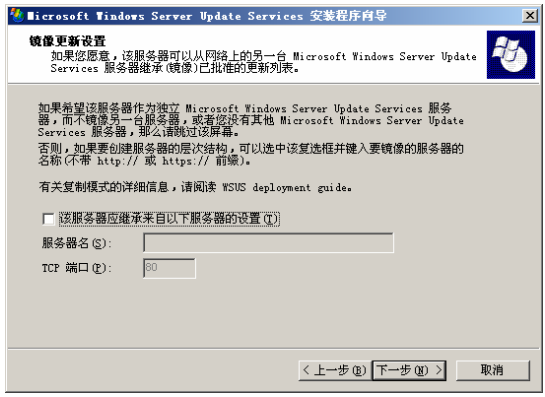

图 13.5 “镜像更新设置”对话框

（4）单击“下一步”按钮，弹出“镜像更新设置”对话框，如图 13.5 所示。如果是新安装 WSUS，不用选择；如果该服务器从已经存在的 WSUS 升级服务器进行更新，选中“该服务器应继承来自以下服务器的设置”，并在“服务器名”文本框输入原 WSUS 升级服务器的 IP 地址。

（5）单击“下一步”按钮，弹出的对话框中显示了摘要信息，包括 WSUS 的内容文件夹、数据库文件路径、管理站点连接地址、客户端自动更新站点和将要安装的组件。

（6）单击“下一步”按钮，将开始安装 WSUS，大约几分钟后，WSUS 完成安装，如图 13.6 所示，选中“启动 Web 管理工具”复选框，单击“完成”按钮，完成安装并启动 WSUS 管理程序。

图 13.6　安装完成

步骤 2：WSUS的设置

WSUS 安装完毕后，打开浏览器，使用地址 http://WSUS_IP/wsusadmin 或 http://WSUS_IP：8530/wsusadmin 访问 WSUS 的管理界面，也可以直接输入计算机名或 IP 地址进行访问，在这里输入 http://192.168.13.246/wsusadmin 进行访问。如果是从其他工作站进入，输入 WSUS 服务器的管理员账户和密码即可成功登录 WSUS 服务器。如图 13.7 所示。此网页显示了 WSUS 的状态，包括 WSUS 已批准的更新、未批准的更新、拒绝的更新、需要更新的计算机、同步状态和待做事项列表等。

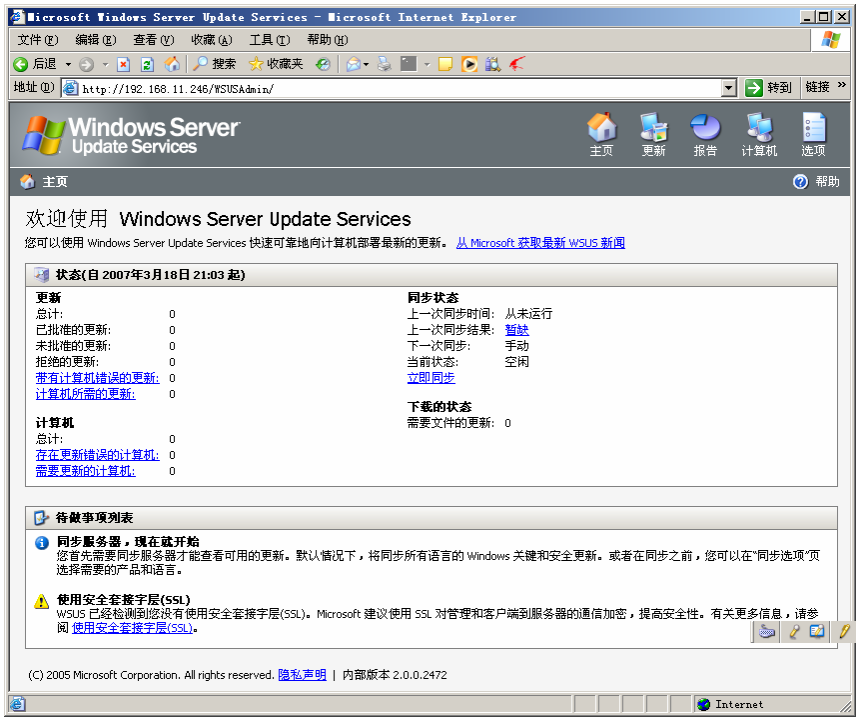

图 13.7　WSUS 主页

单击“选项”图标，进入“选项”窗口。在 WSUS 的“选项”窗口，主要包括 3 部分：同步选项、自动批准选项和计算机选项，如图 13.8 所示。

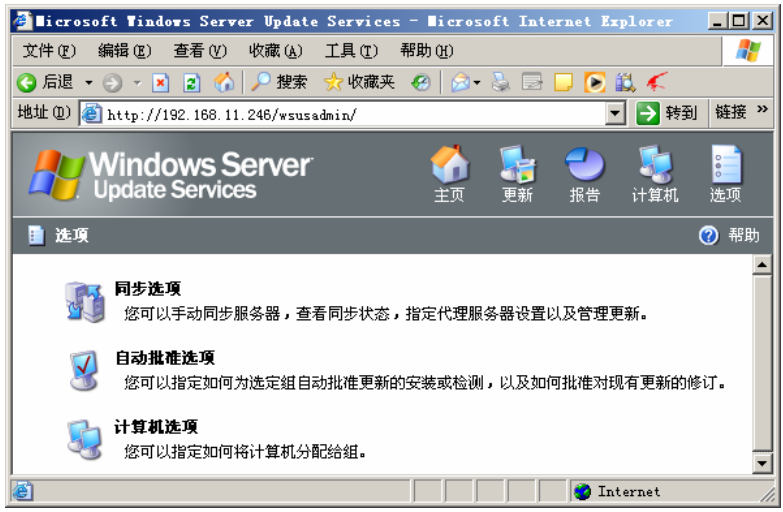

图 13.8　WSUS 选项

1）同步选项

在“同步选项”网页中，有 WSUS 可以更新的产品和分类、WSUS 是否使用代理服务器、WSUS 的更新源和 WSUS 更新的补丁包的语言等选项。如图 13.9 所示。

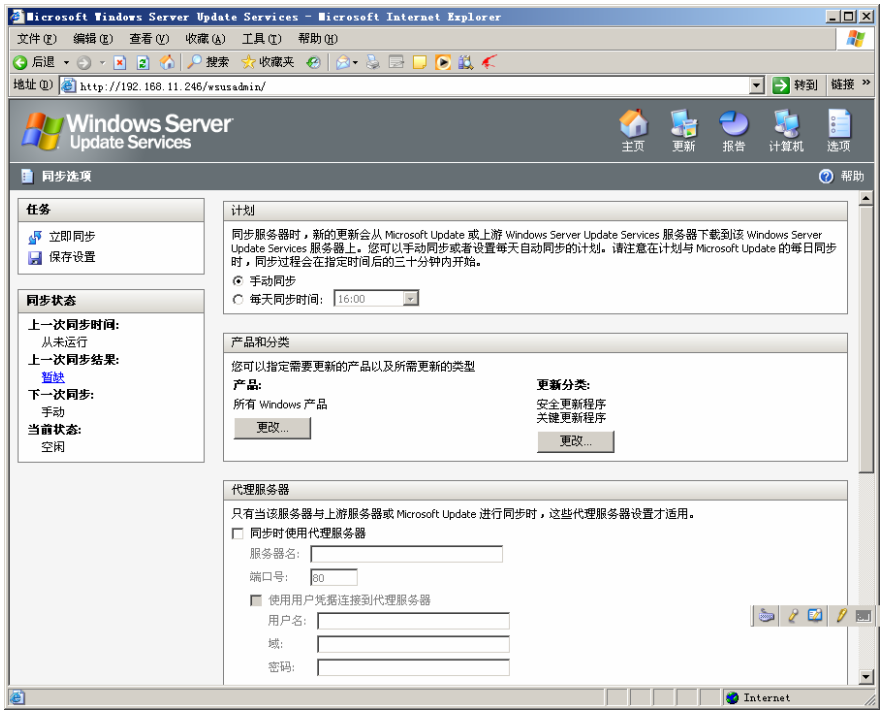

图 13.9　WSUS 同步选项

在“计划”栏中，选择 WSUS 与 Microsoft 升级服务器或 WSUS 与上游 WSUS 同步的方式及时间。通常选择自动同步，并将同步时间设置为网络使用比较少的时刻，如凌晨 0 点到 5 点之间。

在“产品与分类”栏中，选择 WSUS 更新的产品和需要更新的类型。默认情况下，WSUS

只更新所有的 Windows 产品，即 Windows 2000\XP\Server 2003 等操作系统。单击“产品”下的“更改”按钮，选择 WSUS 支持的产品。

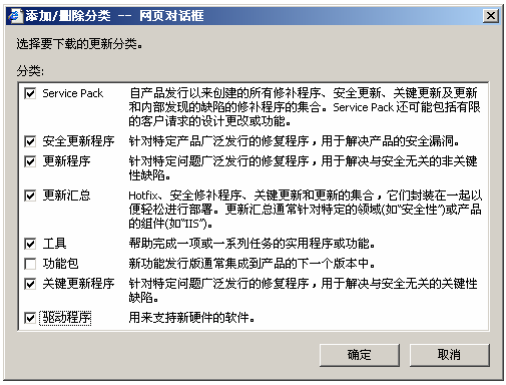

图 13.10　WSUS 更新分类

默认情况下，WSUS 只下载“安全更新程序”和“关键更新程序”，可以在“更新分类”下单击“更改”按钮选择需要下载的更新分类，如图 13.10 所示。

在“代理服务器”栏中，选择 WSUS 与上游服务器或 Microsoft 升级服务器同步时，是否需要使用代理。如果 WSUS 使用 NAT 代理方式或直接上网，则无须设置。

在“更新源”栏中选择 WSUS 更新的方式。如果这是网络中的第一台 WSUS 服务器，则选择“从 Microsoft Update 进行同步”单选按钮；如果网络中已经存在 WSUS，则选择“从上游 Windows Server Update Service 服务器进行同步”单选按钮。并在“服务器名”文本框输入上游 WSUS 服务器的 IP 地址，在“端口号”文本框中输入上游 WSUS 服务器使用的端口号（80 或 8530），如图 13.11 所示。

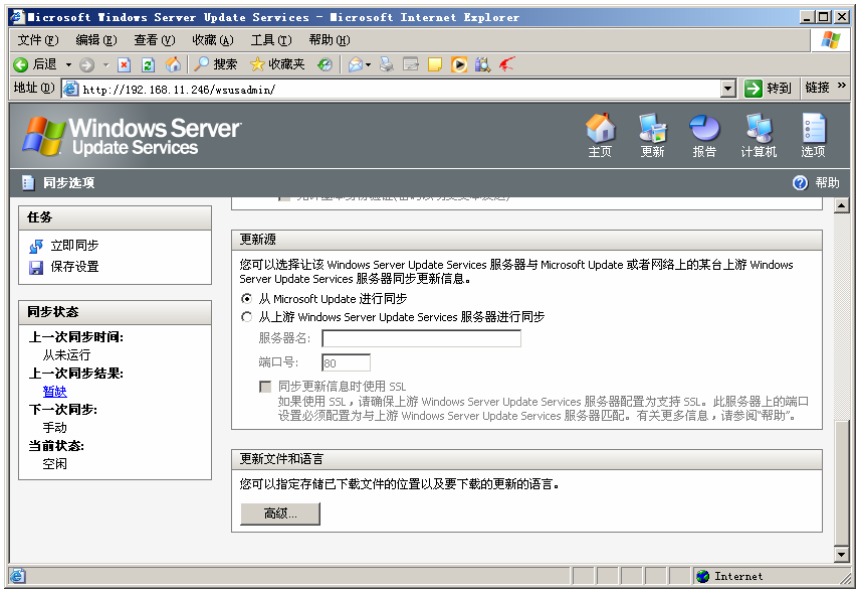

图 13.11　WSUS 更新源

在“更新文件和语言”栏，可以指定 WSUS 下载文件的存储位置和下载的更新语言，单击“高级”按钮进入“高级同步选项”对话框，如图 13.12 所示。

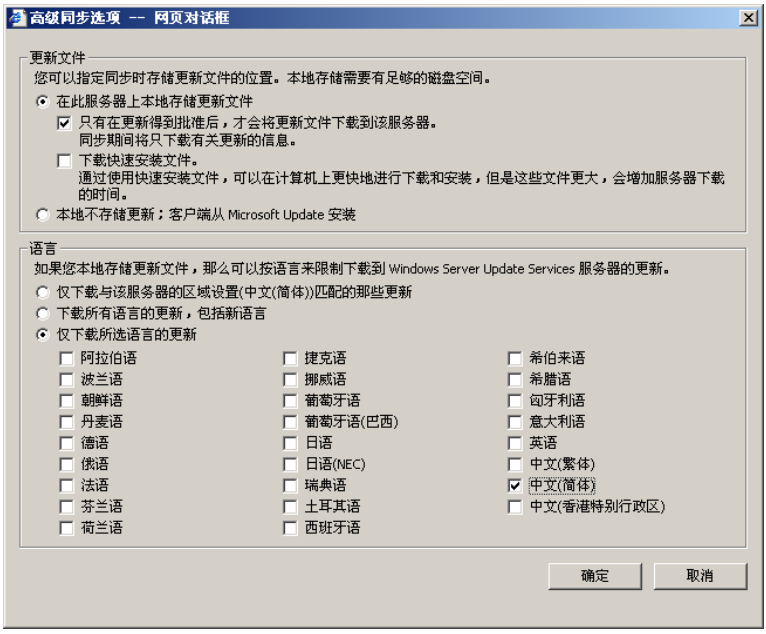

图 13.12　WSUS 高级同步选项

在“更新文件”选项组中，如果选择“只有在更新得到批准后，才会将更新文件下载到该服务器”复选框，则 WSUS 更新时，只下载更新的信息，并不下载更新文件，只有当管理员批准后，才从“更新源”服务器更新。如果只选中“下载快速安装文件”复选框，则 WSUS 不需要管理员批准即下载完全的安装补丁文件。

在“语言”选项组中，选择需要下载的语言。通常情况下，选择“仅下载与该服务器区域设置（中文（简体））匹配的那些更新”单选按钮即可，也可以根据实际情况进行选择，设置之后单击“确定”按钮返回。

之后，单击主窗口左侧“任务”栏中的“保存设置”按钮，保存所做的更改。设置之后，可以单击“任务”栏中的“立即同步”按钮，立即从“更新源”更新补丁。单击右上角的“选项”图标返回。

2）自动批准选项

单击图 13.8 中的“自动批准选项”，弹出“自动批准选项”窗口，如图 13.13 所示。

在“批准进行检测”栏中设置 WSUS 自动批准进行检测的分类。默认情况下包括“安全更新程序”和“关键更新程序”，单击“添加/删除分类”按钮进行更改。

在“批准进行安装”栏中设置 WSUS 自动批准进行安装的分类。默认情况下包括“安全更新程序”和“关键更新程序”，单击“添加/删除分类”按钮进行更改。

默认情况下，在“批准进行检测”和“批准进行安装”栏中的“计算机组”的计算机组为“所有计算机”。

在“更新的修订”栏中，选择“自动批准更新的最新修订”单选按钮。

在“Windows Server Update Service 更新”栏中，选中“自动批准 WSUS 更新”复选框，这样就可以确保正确更新计算机。

之后，单击窗口左侧“任务”栏中的“保存设置”按钮，保存所做的更改。

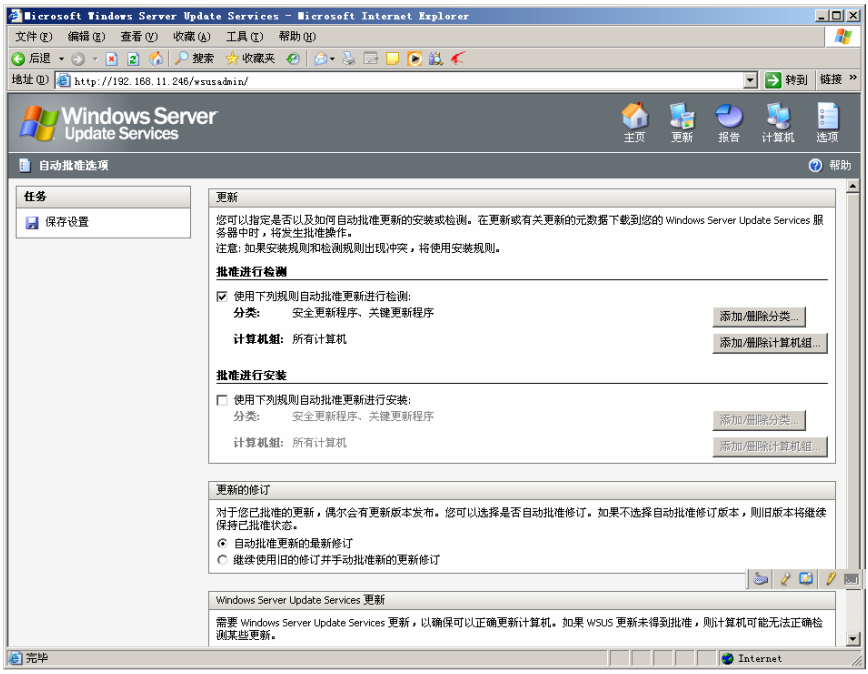

图 13.13　WSUS 自动批准选项

3）计算机选项

单击图 13.8 中的“计算机选项”，弹出“计算机选项”窗口，如图 13.14 所示。

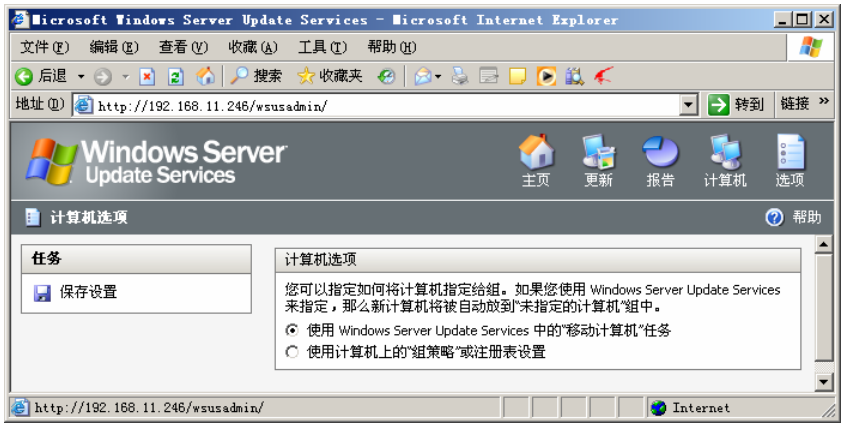

图 13.14　WSUS 计算机选项

选择“使用计算机上的组策略或注册表设置”单选按钮，之后单击窗口左侧“任务”栏中的“保存设置”按钮，保存所做的更改。

4）详细选择 WSUS 支持的产品

设置完成之后，依次单击“选项→同步选项”，打开“同步选项”窗口，单击左侧“任务”栏中的“立即同步”按钮，同步 WSUS。

下载完成后，单击“产品和分类”栏中的“产品”下面的“更改”按钮，可以看到 WSUS 支持的更新，这包括了 Exchange、Office、SQL 和 Windows 系列。如图 13.15 所示。从列表中可以选择需要下载的产品。注意选择完成后单击窗口左侧“任务”栏中的“保存设置”按

钮，保存所做的更改。

图 13.15　选择产品

步骤 3：更新设置

单击“更新”按钮，弹出“更新”窗口，如图 13.16 所示，可以查看 WSUS 下载的更新和更改下载更新的状态。

1）筛选视图

在“筛选的视图”列表中列出了当前的更新数目，在“此服务器上的总计”显示当前 WSUS 服务器上所有的更新数目。可以在窗口左侧的“查看”栏中，选择筛选的条件。

在“产品和分类”下拉列表框中，有“关键与安全更新（所有的关键更新和安全更新）”、“WSUS 更新”和“自定义”3 个选项。

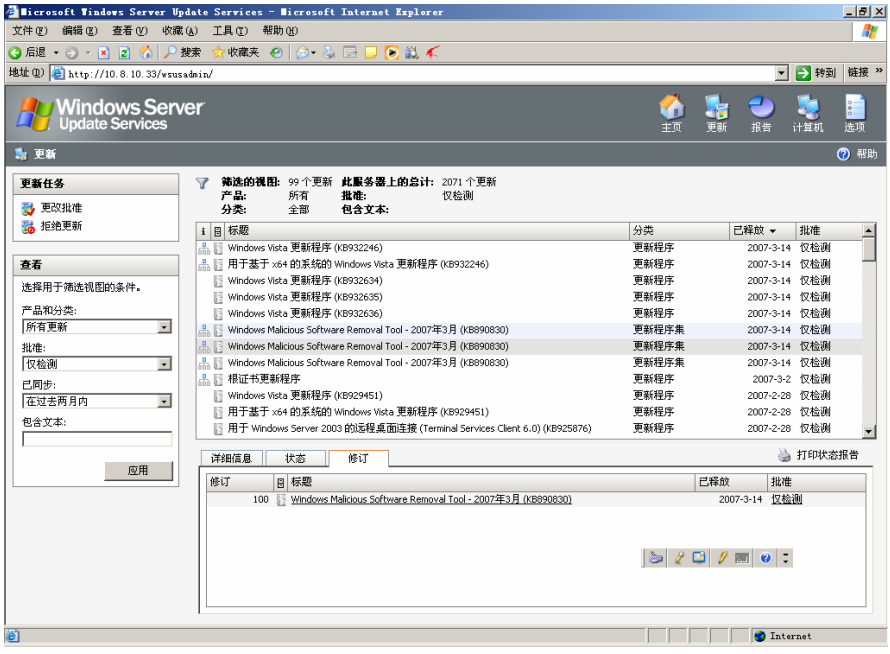

图 13.16　更新窗口

在“批准”下拉列表框中，有“安装（已经批准安装）”、“仅检测（WSUS 检测到的更新）”、“删除（删除的更新）”、“已拒绝（已经拒绝的更新）”、“任何批准（所有批准的更新）”、“未许可（未经许可的更新）”、“所有更新”选项。

在“已同步”下拉列表框中选择更新的时间，包括“上周内”、“在上个月内”等选项。

在“包含文本”文本框中输入更新中包含的文本。

设置完成之后，单击“应用”按钮进行筛选，筛选的条件将是“产品和分类”、“批准”、“已同步”和“包含文本”这 4 个字段中条件的交集。

2）批准所有更新

通常情况下，WSUS 只批准“关键与安全更新”进行安装，可以在“筛选”之后，批准需要的产品进行安装，只有经过批准的安装，WSUS 才从“更新源”进行下载并安装到客户机。

如果要批准所有的更新并允许所有的更新安装到相应的计算机上，操作步骤如下：

（1）在“查看”栏中选择“所有更新”和“任何时间”以列出当前 WSUS 服务器上所有的更新。按住 Shift 键的同时，选择所有的更新，然后单击“更新任务”中的“更改批准”按钮，同意安装所有的更新.

（2）弹出“批准更新→网页”对话框，在“批准”下拉列表框中选择“安装”选项，然后单击“确定”按钮，弹出“Windows Server Update Service 更新－网页”对话框，选择“仅添加新批准项”，然后单击“确定”按钮，此时 WSUS 将开始批准更新的操作。

（3）在“批准安装”之后，WSUS 将从“更新源”下载需要的安装补丁文件。

（4）当所有的补丁下载完成后，即可以为网络中的客户机进行更新。

步骤 4：客户机设置

WSUS 可以为 Windows Server 2000 以上系统的计算机应用更新，在这些系统从 WSUS 获取更新以前，必须进行设置。

1）组策略配置方法

对于加入 Active Directory 的计算机来说，可以通过组策略进行设置；对于没有加入 Active Directory 的计算机来说，可以通过运行“gpedit.msc”命令进行添加设置。

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器的地址，需要在包括网络所有计算机的“组织单元”或其上一级“组织单元”配置组策略，或者将需要更新的计算机“移动”到一个新创建的“组织单元”中，因为指定内部升级服务器的地址，需要在组策略中的“计算机配置”中的“管理模板”→“Windows 组件”→“Windows Update”中进行设置。

如果计算机没有加入 Active Directory 或者想覆盖 Active Directory 中通过组策略指定的 WSUS 升级服务器的地址或配置，可以在客户端计算机上运行“gpedit.msc”命令，并从“计算机配置”中的“管理模板”→“Windows 组件”→“Windows Update”中进行设置。

不论采用何种方式指定，具体设置是一样的。进入组策略编辑器，打开“计算机配置”中的“管理模板”→“Windows组件”→“Windows Update”，双击右边的“配置自动更新”选项，弹出“配置自动更新属性”对话框，如图 13.17 所示，选中自动更新并选择自动更新的方式。如果选择了“自动下载并通知安装”选项，则需要设置“计划安装日期”和“计划安装时间”。然后单击“下一设置”按钮，弹出“指定Intranet Microsoft 更新服务位置属性”对话框，启用内部更新并指定升级服务器的地址，格式为 http://WSUS服务器IP地址，如图 13.18 所示。

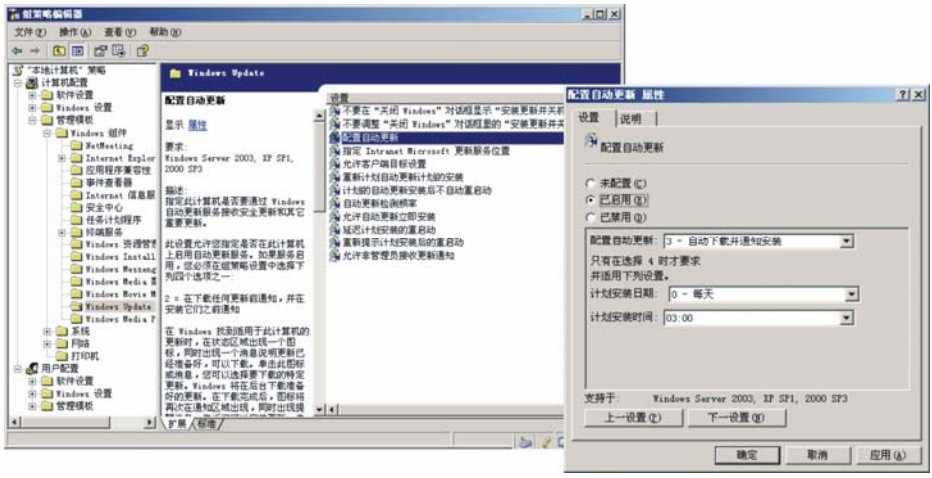

图 13.17　启用自动更新

生效之后，客户机会联系 WSUS 服务器进行升级。

对于 Active Directory 网络中的客户端计算机，需要在组策略刷新之后等待大约 20 分钟。而在默认情况下，每隔 90 分钟计算机组策略便会在后台刷新一次。可以通过运行“gpupdate”命令让设置立即生效，并在客户端计算机通过运行“gpupdate/force”命令立刻生效。

如果是没有加入 Active Directory 的计算机，可能需要通过运行“wuauclt.exe/detectnow”命令来消除 20 分钟延时。

2）客户端安装方法

如果确定系统是 Windows 2000 sp3 以上，或 Windows XP sp1 以上版本可以直接下载以下注册表文件。

使用方法：下载 wsus_cfg.reg 文件后直接单击运行。wsus_cfg.reg 文件内容如图 13.19 所示。

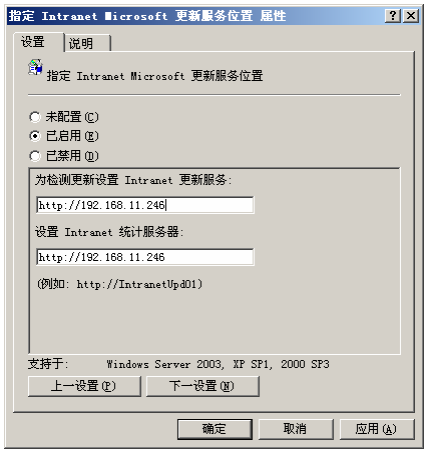

图 13.18　指定 WSUS 服务器地址

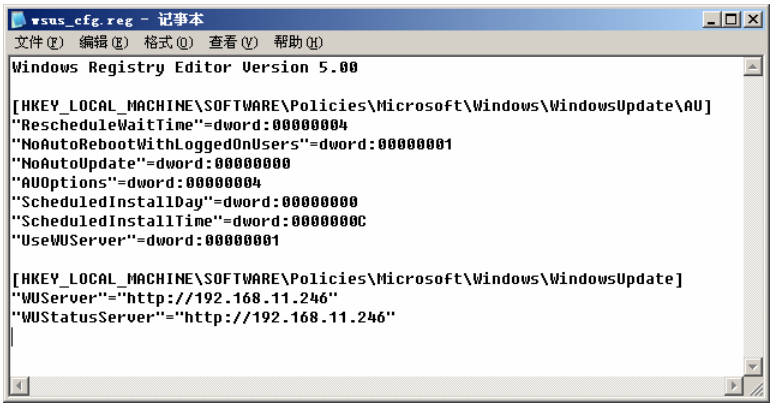

图 13.19　wsus_cfg.reg 文件内容

习　题

一、名词解释

1．WSUS　2．BITS

二、填空题

1．在 Windows Server 2003 系统上，WSUS 安装自带的 MSDE 数据库，通过其数据库保存磁盘至少需要_____的可用空间，如果数据库与 WSUS 下载的补丁在同一分区，则至少需要_____的可用空间。

2．WSUS 支持的更新，包括了_____、_____、_____和 Windows 4 个系列。

3．如果在客户端安装 WSUS，需下载_____文件进行安装。

三、思考题

1．在 WSUS 的“选项”窗口中有哪 3 部分选项，简述各选项的作用。

2．在筛选视图中，有几种条件可供筛选？

3．对加入 Active Directory 的计算机来说，如何通过组策略进行设置 WSUS。

四、实训题

利用微软提供的 WSUS 建立一个内部 Update 服务器，选择一台 Windows 2000 sp3 以上版本系统的计算机，下载 wsus_cfg.reg 文件后直接点击运行，安装并配置一台 WSUS 客户端，让客户端的计算机直接到这台 Update 服务器上实现补丁下载。

项目 14　VPN服务器的配置与管理

14.1　项目内容

1．项目目的

在了解 VPN 概念和熟悉 VPN 工作过程的基础上，学习并掌握在 Windows Server 2003 中 VPN 的安装和基本配置方法。

2．　项目任务

某公司组建了单位内部的办公网络，业务人员经常出差到外地，但需要经常通过公众信息网络访问单位网络，在安全性上存在着很多问题，这时考虑使用 VPN 组网技术解决信息在公众网上传输安全问题。

3．　任务目标

① 了解 VPN 的概念；
② 理解 VPN 的工作过程；
③ 掌握如何在 Windows Server 2003 中安装与配置 VPN 服务；
④ 客户端 VPN 连接的设置。

14.2　相关知识

如何在异地安全地访问本地网络是网络应用中常遇到的问题，如出差在外的工作人员或派外地的办事机构，他们可能需要异地的连接公司的内部网络来获取一些信息等。这类应用的特点一是要求安全访问内部网络；二是要求异地访问能够像本地访问一样运行数据库客户端软件，甚至浏览共享文件夹。

14.2.1　VPN的概念

虚拟专用网（Virtual Private Network，VPN）技术是通过 ISP（Internet 服务提供商）和其他 NSP（网络服务提供商）在公用网络中建立专用的数据通信网络的技术。虚拟专用网虽不是真的专用网络，但却能够实现专用网络的功能。虚拟是指用户不必拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。在虚拟专用网络中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理网络，数据通过安全的加密管道在公共网络中传播。虚拟专用网可以实现不同网络的组件和资源之间的相互连接，能够利用 Internet 或其他公共互联网的基础设施为用户创建隧道，并提供与专用网络相同的安全和功能保障。

14.2.2　VPN服务的原理

VPN 服务的原理如图 14.1 所示，VPN 客户机可以利用电话线路或者 LAN 接入本地

Internet。当数据在 Internet 上传输时，利用 VPN 协议对数据进行加密和鉴别，这样，VPN 客户机和服务器之间经过 Internet 的传输好像是在一个安全的“隧道”中进行。通过“隧道”建立的连接就像专门的网络连接一样，这就是虚拟专用网络的含义。

图 14.1　VPN 服务原理

在 TCP/IP 协议中，对数据进行封装的过程如图 14.2 所示。VPN 技术就是在网络层对数据进行加密的一种技术，称为隧道方式的加密和鉴别技术，其数据报文如图 14.3 所示。

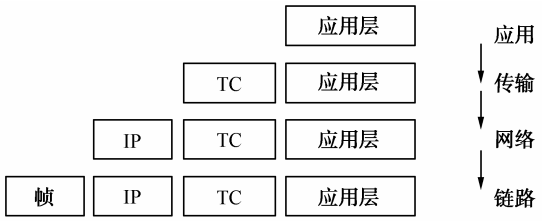

图 14.2　TCP/IP 网络的数据报文封装流程

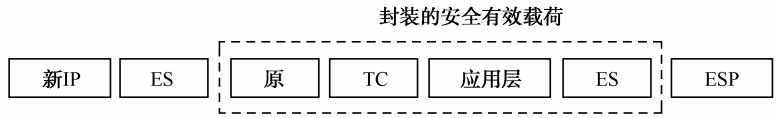

图 14.3　VPN 技术的数据报文

14.2.3　VPN的类型

1．客户端发起的VPN

远程客户通过 Internet 连接到企业内部网，通过网络隧道协议与企业内部网建立一条加密的 IP ，从而安全地访问内部网的资源。

在这种方式下，客户机必须维护和管理发起隧道连接的有关协议和软件。

2．接入服务器发起的VPN

远程客户接入本地 ISP 的接入服务器后，接入服务器发起一条隧道连接到用户需要连接的企业内部网，构建 VPN 所需的软件和协议均由接入服务器来提供和维护。

14.2.4　VPN的隧道协议

VPN 使用隧道协议来加密数据，目前主要使用 4 种隧道协议：PPTP（点对点隧道协议）、L2TP（第二层隧道协议）、网络层隧道协议 IPSec 及 Socks V5。它们在 OSI 七层模型中的位置如表 14.1 所示。各协议工作在不同层次，在选择 VPN 产品时，应注意不同的网络环境适合不同的协议。

表 14.1　4 种隧道协议在 OSI 模型中的位置

OSI 七层模型	安全技术	安全协议
应用层	应用层代理	
表示层		
会话层	会话层代理	SocksV5
传输层		
网络层	包过滤	IPSec
数据链路层		PPTP / L2TP
物理层		

1．PPTP

PPTP（Point to Point Tunning Protocol，点到点隧道协议）是在 Window95/98 中支持的，为中小企业提供的一个 VPN 解决方案。PPTP 是在 PPP（点对点协议）的基础上开发的新的增强型安全协议，可以使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网。通过使用 PPTP 可以增强 VPN 连接的安全性，例如，可对 IP、IPX 或 NetBEUI 数据流进行 40 位或 128 位加密，然后封装在 IP 包中，通过企业 IP 网络或公共互联网发送到目的地。另外，使用 PPTP 还可以控制网络流量，减少网络堵塞的可能性。但 PPTP 性能不高，目前，PPTP 协议在 VPN 产品中使用较少。

2．L2TP协议

L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）是 Microsoft 的 PPTP 和 Cisco 的 L2F（Layer 2 Forwarding，第二层转发）的组合，该技术由 Cisco 公司首先提出，指在 IP、X.25、帧中继或 ATM 网络上用于封装所传送 PPP 帧的网络协议。以数据报传送方式运行 IP 时，L2TP 可作为 Internet 上的隧道协议。L2TP 还可用于专用的 LAN 之间的网络。它同样适用于非 IP 协议，支持动态寻址，是目前唯一能够提供全网状 Intranet VPN 连接的多协议隧道。

3．IPSec协议

IPSec 是一组开放的网络安全协议的总称，提供访问控制、无连接的完整性、数据来源验证、防重放保护、加密及数据流分类加密等服务。 IPSec 在 IP 层提供这些安全服务，它包括两个安全协议 AH（报文验证头协议）和 ESP（报文安全封装协议）。AH 主要提供的功能有数据来源验证、数据完整性验证和防报文重放功能。ESP 在 AH 协议的功能之外再提供对 IP 报文的加密功能。AH 和 ESP 同时具有认证功能，IPSec 存在两个不同的认证协议是因为 ESP 要求使用高强度密码学算法，而高强度密码学算法在很多国家都存在很多严格的政策限制。但认证措施是不受限制的，因此 AH 可以在全世界自由使用。另外一个原因是很多情况下人们只使用认证服务。AH 或 ESP 协议都支持两种模式的使用：隧道模式和传输模式。隧道模式对传经不安全的链路或 Internet 的专用 IP 内部数据包进行加密和封装（此种模式适合于有 NAT 的环境）。传输模式直接对 IP 负载内容（即 TCP 或 UDP 数据）加密（适合于无 NAT 的环境）。

4．Socks V5 协议

Socks V5 协议工作在会话层，它可作为建立高度安全的 VPN 的基础。Socks V5 协议的优势在访问控制，因此适用于安全性较高的 VPN。该协议最适合于客户机到服务器的连接模

式，适用于外部网 VPN 和远程访问 VPN。

14.2.5 VPN的应用

1．以安全方式，通过 Internet 实现访问企业局域网。

2．通过 Internet 实现网络互连，分别可以采用专线连接和拨号连接，这样就可以将与当地 ISP 建立的连接和 Internet 网络在企业分支机构和企业端路由器之间创建一个 VPN。

3．连接企业内部网络计算机，通过使用 VPN 服务器来与整个企业局域网连接，并可保证数据的安全性。

14.3 方案设计及准备

1．设计

任务要求如下。

（1）VPN 服务器安装双网卡，内网设置一个私有 IP：10.8.32.0/24，连接公司内网。外网设置一个可以连接到 Internet 的公有 IP：211.81.192.2/24。

（2）远程客户端需要连接到 Internet 上。然后通过在 Internet 上建立虚拟专用通道连接到公司内部网络的 VPN 服务器上，即建立一个虚拟专用连接，可以自由访问内部网络。网络拓扑图如图 14.4 所示。

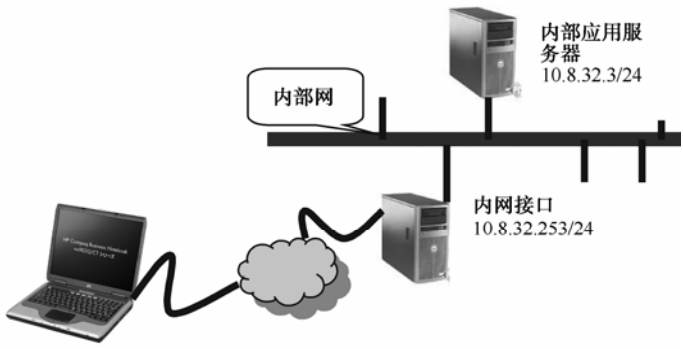

图 14.4 网络拓扑结构图

2．设备清单

为了搭建图 14.4 所示的网络环境，需要如下设备：

① 安装 Windows Server 2003 的 PC 计算机 1 台；

② 安装 Windows XP 的计算机 1 台；

③ 以上计算机已连入校园网。

14.4 项目实施

步骤 1：配置VPN服务器的网卡IP地址

在安装 Windows Server 2003 VPN 服务器之前，需要安装所有硬件并使其正常工作。首先要

设置两块网卡（连接内网的网卡和连接外网的网卡）的属性，分别在 TCP/IP 属性对话框中，输入 IP 地址、子网掩码等信息，默认网关不必设置或设置为本机的 IP 地址，如图 14.5、图 14.6 所示。

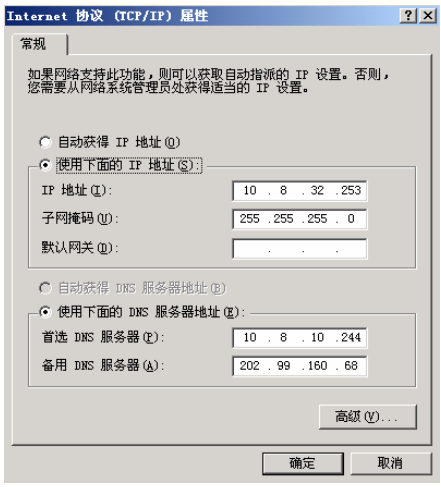

图 14.5　连接内网网卡 TCP/IP 设置

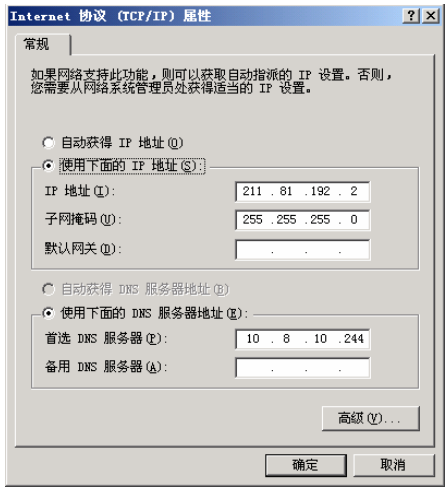

图 14.6　连接外网网卡 TCP/IP 设置

步骤 2：安装和启动VPN服务器

使用 Windows Server 2003 安装 VPN 服务器，具体的操作步骤如下。

（1）启动“路由和远程访问”管理应用程序。选择“开始→程序→管理工具→配置你的服务器向导”命令，弹出“配置你的服务器向导”对话框，单击“下一步”按钮，弹出“预备步骤”对话框，单击“下一步”按钮，弹出“服务器角色”对话框，如图 14.7 所示。

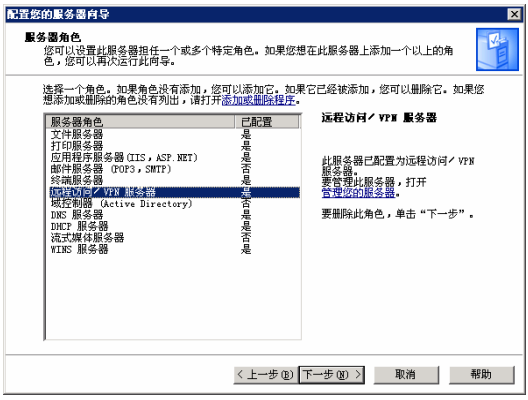

图 14.7　“服务器角色”对话框

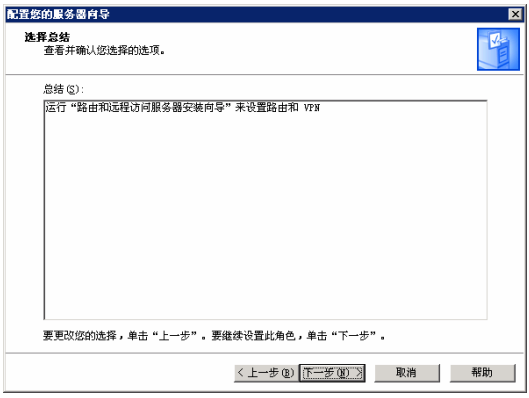

图 14.8　“选择总结”对话框

（2）选择“远程访问/VPN 服务器”选项，单击“下一步”按钮，弹出“选择总结”对话框，如图 14.8 所示。

（3）单击“下一步”按钮，弹出“路由和远程访问服务器安装向导”对话框。单击“下一步”按钮，弹出“配置”对话框，如图 14.9 所示，单击“远程访问（拨号或 VPN）”选项，允许远程客户端通过拨号或安全的虚拟专用网络连接到此服务器。

（4）单击“下一步”按钮，弹出“远程访问”对话框，如图 14.10 所示，根据应用模式选择服务器的角色，选择“VPN”或“拨号”，这里选择“VPN”。

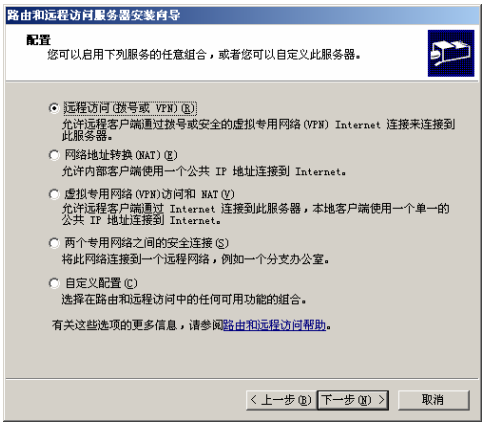

图 14.9 “配置”对话框

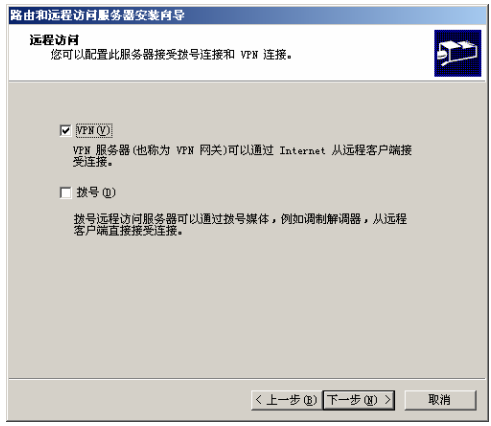

图 14.10 “远程访问”对话框

（5）配置远程访问服务器网络接口地址。单击“下一步”按钮，弹出“VPN 连接”对话框，如图 14.11 所示，显示连接到 Internet 的网络接口和内网接口。

（6）对远程客户指派 IP 地址。单击“下一步”按钮，弹出“IP 地址指定”对话框，如图 14.12 所示，如果要使用 DHCP 服务器（参见 DHCP 章节内容）给远程客户端分配地址，在 IP 地址指定设置对话框中选择“自动”单选按钮；如果给远程客户端分配静态 IP 地址，选择“来自一个指定的地址范围”。采用 DHCP 管理分配 IP 地址更简单方便，但若网络中没有安装 DHCP 服务，则必须指定一个地址范围。

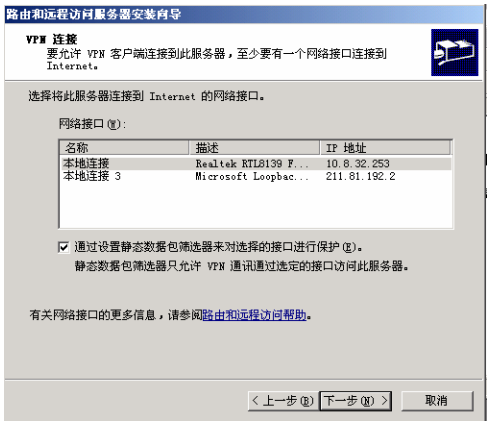

图 14.11 “VPN 连接”对话框

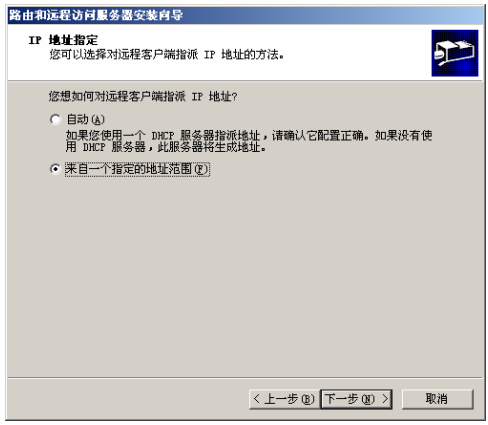

图 14.12 “IP 地址指定”对话框

（7）单击“下一步”按钮，弹出“地址范围指定”对话框，如图 14.13 所示，单击“新建”按钮，指定“起始 IP 地址”和“结束 IP 地址”。Windows 将自动计算地址的数目。单击“确定”按钮返回到地址范围分配窗口，如图 14.13 所示。本例中为远程访问客户分配了从 10.8.32.3 至 10.8.32.15 共 20 个 IP 地址。远程访问客户在 VPN 客户端设置时，可以选择该范围中的任何一个 IP 地址分配。

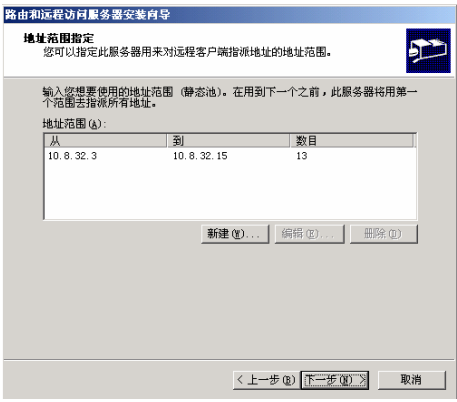

图 14.13　IP 地址范围的设定

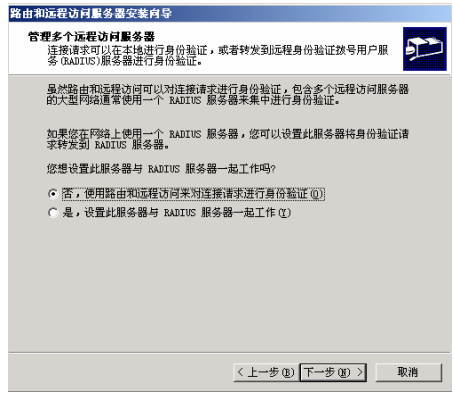

图 14.14　身份验证模式对话框

（8）单击“下一步”按钮，弹出“管理多个远程访问服务器”对话框，如图 14.14 所示，选择默认选项“否，使用路由和远程访问对连接请求进行身份验证”，此时远程访问用户使用本服务器中管理的用户账号连接本 VPN 服务器，并且该账号已经授予远程访问权限。如果网络中存在 RADIUS 服务器，可以集成该服务器验证远程访问客户。

（9）单击“下一步”按钮，弹出“完成”对话框，单击“完成”按钮，结束安装。系统启用路由和远程访问服务并将该服务器配置为远程访问服务器。

步骤 3：配置 VPN 服务器

VPN 服务器安装完成后，可以进行配置，保证远程用户顺利连接 VPN 服务器。

1）配置远程访问策略

通过配置远程访问策略可以修改指派远程用户 IP 作用域，授权或拒绝远程用户的访问。配置远程访问策略的步骤如下：

① 选择“开始→程序→管理工具→路由和远程访问”命令，打开“路由和远程访问”窗口，如图 14.15 所示。

② 在图 14.15 中，选择本地远程访问服务器 MA，单击“远程访问策略”，在右边窗口中右击“到 Microsoft 路由选择和远程访问服务器的连接”，在弹出的快捷菜单中选择“属性”选项，弹出“到 Microsoft 路由选择和远程访问服务器的连接属性”对话框，如图 14.16 所示。

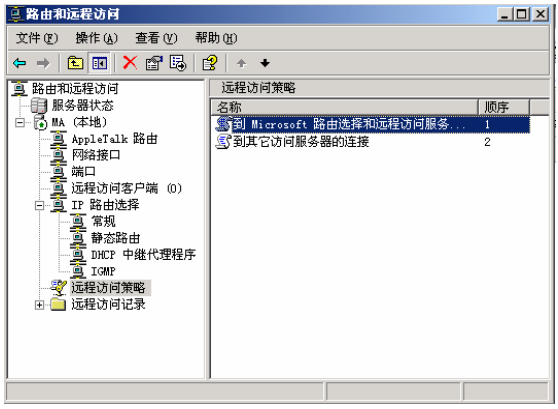

图 14.15　配置远程访问策略

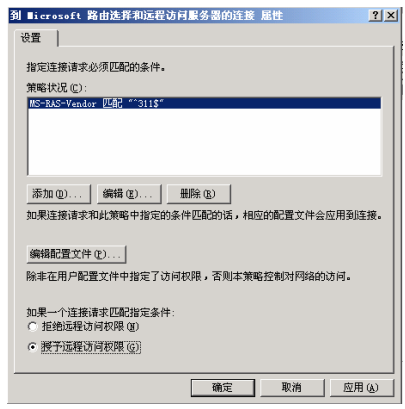

图 14. 16　授予远程访问权限

③ 在图 14.16 中，可以对远端客户端的远程访问权限进行设置，如果允许远程客户端通

过 Internet 访问该服务器，则选择“授予远程访问权限”；反之，选择“拒绝远程访问权限”。如果还需要对配置文件进行设置，单击“编辑配置文件”按钮，出现如图 14.17 所示“编辑拨入配置文件”对话框。

④ 在“编辑拨入配置文件”对话框中单击 IP 选项卡，根据需要选择 IP 地址的分配。共有 4 种选择，其含义如下：

选择“服务器必须提供一个 IP 地址”选项，则需要在用户“属性”对话框中给远程登录用户配置一个静态的 IP 地址，用户属性配置参见用户管理，分配给用户的静态 IP 地址如图 14.18 所示。

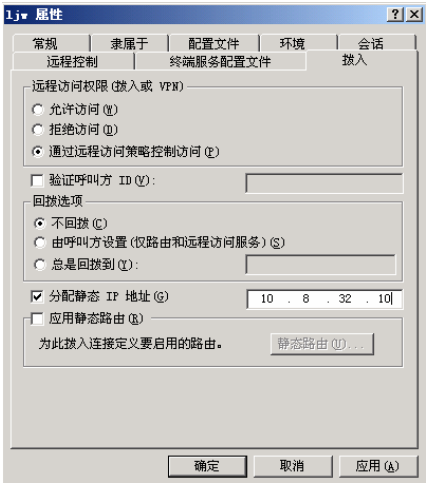

图 14.17 所示“编辑拨入配置文件”

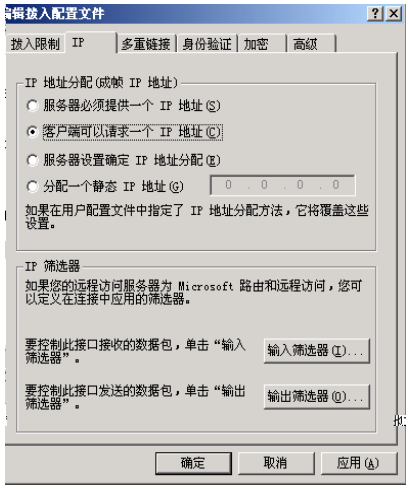

图 14.18 分配给用户静态 IP 地址

- 选择“客户端可以请求一个 IP 地址”选项，VPN 客户可以设置使用 VPN 服务器地址池中的任意 IP 地址，此时 VPN 用户拥有固定的内网 IP 地址。
- 选择“服务器设定 IP 地址分配”选项，VPN 客户端无须配置内部网络 IP 地址，VPN 客户端软件连接 VPN 服务器时，自动从 VPN 服务器的 IP 地址池中获取一个内部 IP 地址。
- 选择“分配一个静态 IP 地址”选项，VPN 服务器只为 VPN 客户端提供一个固定的 IP 地址，因此，一个时刻只允许远端一台客户机登录 VPN 服务器。

对上述内容设置完成后单击“确定”，完成对“远程访问策略”的设置。

2）修改同时连接的数目

对于 VNP 客户连接的用户数目可以进行限制，默认情况下允许 128 个连接。若要更改同时连接的数目，启动“路由和远程访问”应用程序。选择服务器对象（MA），右击“端口”，选择“属性”菜单项。在“端口属性”对话框中，单击“WAN 微型端口（PPTP）”，然后单击“配置”按钮，打开“配置设备 WAN 微型端口（PPTP）”对话框，如图 14.19 所示。

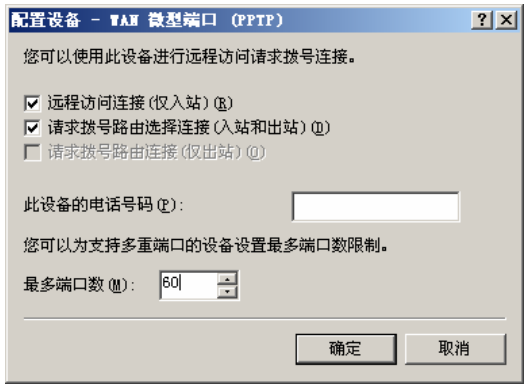

图 14.19　设置连接“最多端口数”

设置“最多端口数”，输入允许同时连接的端口数目，单击“确定”按钮完成配置。

3）配置用户的属性

对于允许远程连接的用户账户必须设定其“允许远程访问”，具体步骤如下：

① 选择“开始→控制面板→管理工具→计算机管理”命令，打开“计算机管理”窗口，选择“本地用户和组”，单击“用户”。如图 14.20 所示。

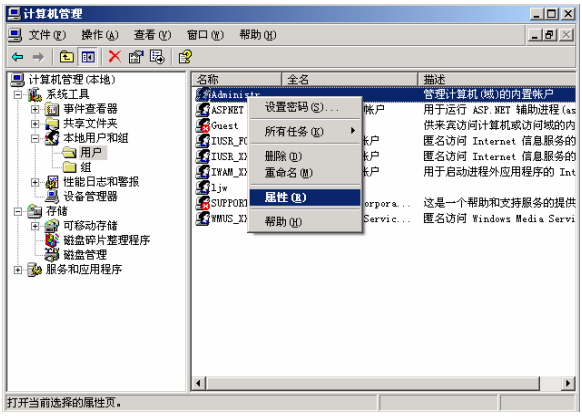

图 14.20　设置用户属性

② 在用户窗口中选择要设置的用户，鼠标右击用户，选择“属性”菜单项。

③ 在出现的“属性”窗口中单击“拨入”选项卡，然后在出现的如图 14.21 所示窗口中，选择“允许访问”或“通过远程访问策略控制访问”，则该用户具有远程连接权力。反之，不允许用户远程访问该服务器。若选择“通过远程访问策略控制访问”，则需要按前面的步骤配置“远程访问控制策略”。单击“确定”按钮完成设置。

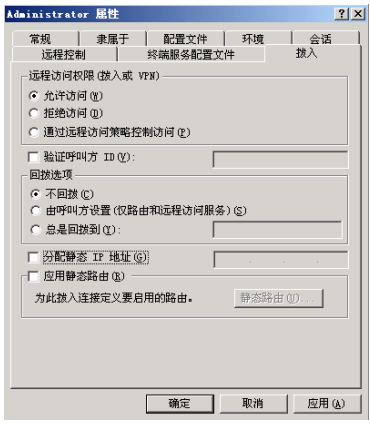

图 14.21　设置用户远程访问属性

步骤 4：配置客户端的 VPN连接

VPN 客户端既可以通过拨号，也可通过局域网的形式访问 VPN 服务器。下面介绍在运行 Windows XP 的客户机

上通过局域网的形式访问 VPN 服务器的具体步骤。

（1）在 VPN 客户机上新建一个网络连接。选择“开始→设置→控制面板→网络连接”命令，打开“网络连接”窗口，选择“文件→新建连接”命令，弹出“新建连接向导”对话框。

（2）单击“下一步”按钮，弹出“网络连接类型”对话框，如图 14.22 所示，选中“连接到我的工作场所的网络”单选按钮。

（3）单击“下一步”按钮，弹出“网络连接”对话框，如图 14.23 所示，选中“虚拟专用网络连接”单选按钮。

（4）单击“下一步”按钮，弹出“连接名”对话框，如图 14.24 所示，在公司名称对话框中为连接输入一个描述性的名称，即对公司名称的一个简单描述，如 XPC。

（5）单击“下一步”按钮，弹出“VPN 服务器选择”对话框，如图 14.25 对话框，输入目标地址即 VPN 服务器的 IP 地址或主机名。

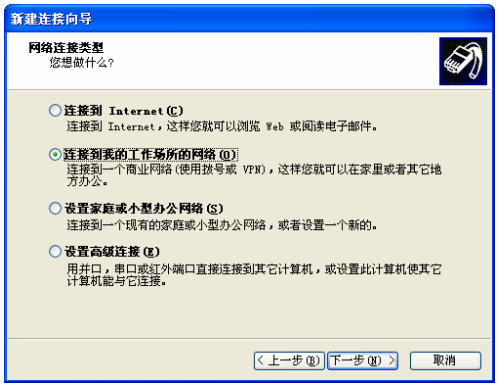

图 14.22　创建一个新的连接

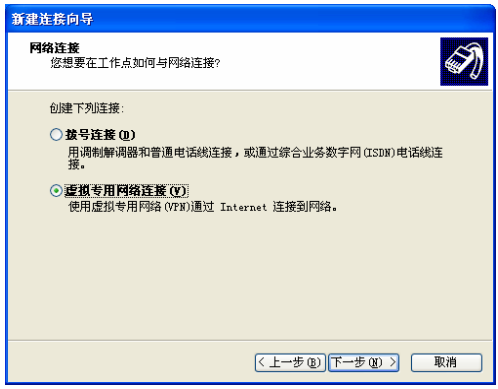

图 14.23　输 VPN 服务器的 IP 地址

（6）单击“下一步”按钮，弹出“正在完成新建连接向导”对话框，单击“完成”按钮，保存新建的连接。

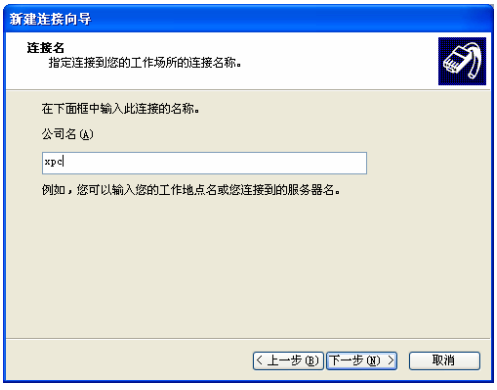

图 14.24　“连接名”对话框

图 14.25　“VPN 服务器选择”对话框

步骤 5：建立与VPN服务器的连接

当用户需要与远程 VPN 服务器连接时，可以运行上面建立的虚拟专用连接。

当计算机向 VPN 服务器请求连接时，系统提示输入用户名和密码，如图 14.26 所示。输

入登录 VPN 服务器的用户名和密码，单击“连接”按钮。

若成功连接，则会出现如图 14.27 所示的对话框，单击“确定”按钮即可，这时用户就可以像访问本地计算机一样访问远端内部网络。

图 14.26　连接虚拟专用网

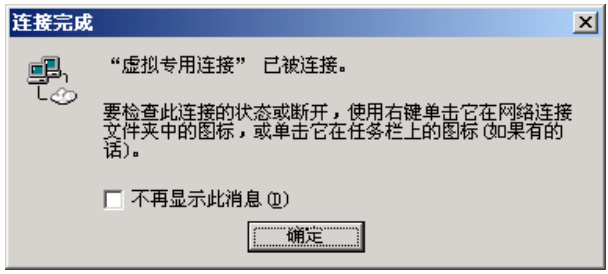

图 14.27　虚拟专用连接成功

若连接失败，则根据不同的情况，会出现不同的连接错误提示对话框。例如，如果出现图 14.28 所示对话框，原因可能有下面几个方面：

图 14.28　虚拟连接失败

① 用户远程连接属性被设置为“拒绝访问”；

② 远程策略里设置“拒绝远程访问权限”；

③ 远程访问策略里配置文件设置错误等。

此时用户可以仔细检查用户属性，包括用户名和密码的正确性、远程访问属性设置的正确性，以及远程访问策率的配置的正确性。

习　题

一、填空题

1．VPN 使用隧道协议来加密数据，目前主要使用_____、_____、_____以及_____4 种隧道协议。

2．L2TP 协议是 Microsoft 的_____和_____的 L2F 的组合。

3．IPSec 在 IP 层提供这些安全服务，它包括两个安全协议_____和_____。

二、选择题

1．下面哪项是目前唯一能够提供全网状 Intranet VPN 连接的多协议隧道（　　）。

A．PPTP 协议　　B．L2TP 协议

C. IPSec 协议　　D. Socks V5 协议

2．以下哪一项不属于 ISO 七层模型（　　）。

A. 链路层　　B. 会话层

C. 协议层　　D. 物理层

三、思考题

1．什么是虚拟专用网？

2．VPN 服务的原理是什么？

3．简述拨号连接和虚拟专用连接的区别与联系？

4．如何从客户端进行 VPN 连接？

四、实训题

1．安装并配置一台 Windows Server 2003 VPN 服务器，允许远程客户端通过 Internet 访问该服务器，则选择“授予远程访问权限”，单击“编辑配置文件“按钮，选择“客户端可以请求一个 IP 地址”选项设置 VNP 客户连接的用户数目为 60 个连接。

2．配置一个 VPN 客户端，并建立与 VPN 服务器的连接。

项目 15　Windows Server 2003 性能监视和优化

Windows Server 2003 系统提供了功能强大的可用于对系统的资源和信息进行实时监控的“系统监视器”，以评估计算机的性能。不仅可以收集并查看本地计算机的信息，而且可以通过网络获得远程计算机上的实时性能数据。在 Windows Server 2003 中，为了提高系统的安全性，新增了“performance Log Users”和“performance Monitor Users”两个安全组，用于确保只有受信任的用户才可访问和操作敏感的性能数据。

Windows Server 2003 提供了诸多的可管理模块，其中最常用也是最重要的几个监控模块为：

- 系统监视器；
- 性能日志和警报；
- 任务管理器；
- 网络监视器。

15.1　项目内容

1．项目目的

掌握在 Windows Server 2003 系统中熟练使用系统监视器、性能日志、任务管理器、网络监视器的方法。

2．项目任务

在安装 Windows Server 2003 系统的计算机上通过使用任务管理器来监视系统进程，观测计算机性能。

3．任务目标

① 掌握系统监视器的使用；
② 掌握任务管理器的使用；
③ 掌握网络监视器的使用配置。

15.2　实施步骤

15.2.1　使用性能监视器

系统监视器能监视系统的性能，是维护和管理操作系统的重要组成部分。系统监视器在默认情况下对内存、硬盘及 CPU 的运行状况进行监视，网络管理员可以对显示方式、数据来源和外观进行调整，满足监控的需要。下面介绍系统监视器的设置。

选择“开始→设置→控制面板→管理工具→性能”命令，打开“性能”对话框，如图 15.1

所示。在“性能”窗口左边窗格中可看到“系统监视器”和“性能日志和警报”两项管理单元，在“性能日志和警报”下又包含 3 个记录日志，分别为计数器日志、跟踪日志和警报。

- 系统监视器：是性能监视器的重要组成部分，其主要功能是收集并查看本地计算机或远程计算机的即时性能数据，以及查看计数器日志中当前或以前已经收集的资料等。
- 性能日志：用来收集关于硬件资源、系统服务及性能的数据。
- 警报：是在各项指标超出设定标准时，系统用以通知用户或管理员的工具。

在“性能监视器”窗口中，右边的窗格中显示了监视器的工具栏和图表，下面是计数器。图表区域起初是空白的，将计数器加入图表后，“性能监视器”开始在图表区域绘制计数值图表。

系统监视器中的计数器区域显示了包括颜色、比例、计数器、实例、父系、对象及计算机等相关信息，其中最主要的信息为：

- 对象。是指计算机系统的组件或子系统，如硬件或软件。
- 实例。是指相同类型的多个对象。例如，系统有多个处理器，Processor 对象类型就有多个。
- 计数器。是对象的属性，是采集数据的主要工具。例如，对于 Processor 对象，计数器收集处理器时间和用户时间的数据。不管数据在“系统监视器”中是否可见，内置在操作系统中的计数器总是不断地捕获数据。如果一个对象类型有多个实例，计数器会跟踪每个实例的统计数据。

步骤 1：设置显示方式

系统性能监视器能提供 3 种不同的显示方式。

默认状态下，性能以图表视图方式显示。单击工具栏中的相应按钮，可以以直方图或报告视图方式显示。

（1）图表视图用线性图表格式显示一段时间内的计数器数据，是一种以时间为横坐标、监视值为纵坐标的坐标系，用相应曲线的变化来反映实时资源的运行情况，在同时监视多个不同的参数时，可以使用不同的颜色分别表示。

（2）直方图视图可按条形图格式显示计数器数据，每个计数器实例仅显示一个数值。如图 15.2 所示。

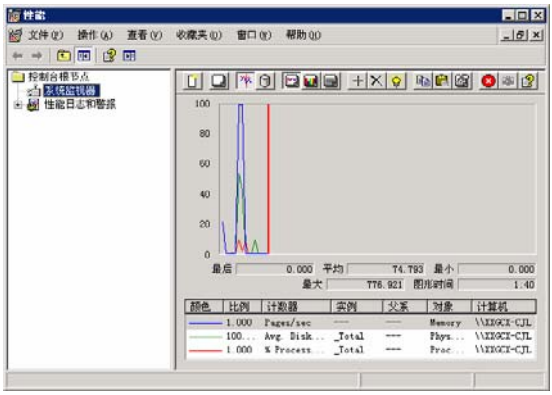

图 15.1 “性能”窗口

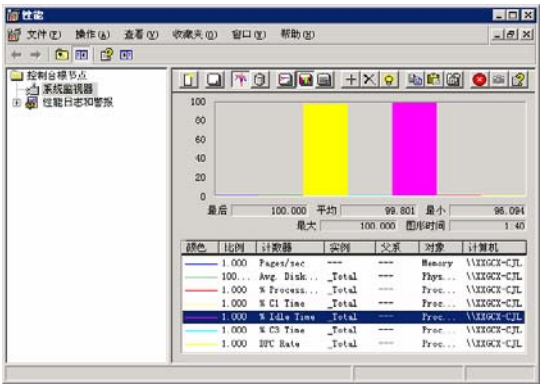

图 15.2 直方图方式

（3）报告视图可按表格形式显示计数器数据，每个计数器实例仅显示一个数值。在报告

视图中，计数器名称和数据数值显示在与之相关联的性能对象下面的行中，每个实例及其数据显示在单独的列中。

步骤 2：设置默认视图与采样方式

选择“常规”选项卡，如图 15.3 所示，在“查看”栏中可以指定显示类型，在“显示元素”栏选择视图的具体样式。在“报告和直方图数据”栏中，如果选择平均值、最小值或最大值统计信息，就会在每个采样间隔中计算统计信息。但这会为实时数据带来额外的性能开销。另外，还可指定所需的采样选项。若以定期间隔自动采样，可选中“自动采样间隔”复选框，并在“秒”文本框中输入间隔时间（秒），默认间隔为 1 秒。若欲手动采样，应当清除“自动采样间隔”复选框。在选择手动采样时，应使用“更新数据”按钮来收集采样。

步骤 3：设置数据来源

单击工具栏中的“查看日志数据”按钮，或者在图表中右击，并在快捷菜单中选择“属性”命令，打开“系统监视器属性”对话框，如图 15.4 所示。在“来源”选项卡中，选择“当前活动”选项，显示当前活动的性能情况，还可以选择“日志文件”或“数据库”选项，用于显示历史性能情况。

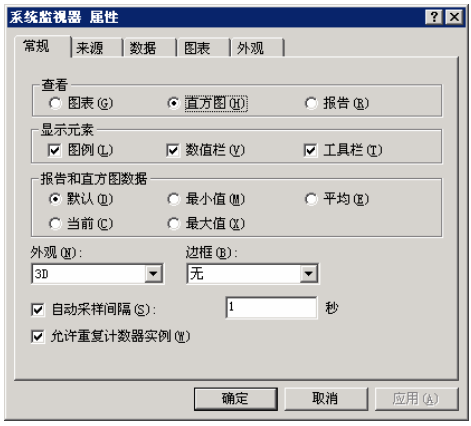

图 15.3　“常规”选项卡

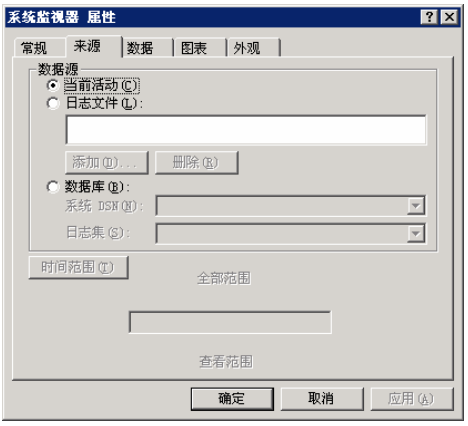

图 15.4　“来源”选项卡

步骤 4：设置视图外观样式

选择“外观”选项卡，如图 15.5 所示，可更改背景、图表、文本和字体属性。若欲更改颜色元素，先在“颜色”下拉列表框中选择想要更改其颜色的图形元素，单击“更改”按钮，并在“颜色”对话框中选择颜色。“颜色”中的可用元素有如下几种。

图表背景：计数器数据图表的窗口区域的背景颜色。

控制背景：环绕数据图表的窗口区域的背景颜色。

文本：文本颜色。

网格：垂直或水平网格线条所用的颜色。

时间栏：计时器栏所用的颜色。

若欲更改图形上的文本或数字所用的字体，在“字体”栏中单击“更改”按钮，然后设置想要的任何字体选项。选项包括“字体”、“字形”、“大小”和“字符集”。

步骤 5：设置计数器

计数器是收集系统性能数据的主要工具，所以要在“系统监视器”中添加计数器，这样用户就可以监视系统的性能。

选择“数据”选项卡，如图 15.6 所示，可更改计数器和计数器属性。默认情况下，“系统监视器”会显示本机的 Pages/sec、Avg.Disk Queue Length、% Processor Time 计数器的数据。

图 15.5 “外观”选项卡

图 15.6 “数据”选项卡

单击“添加”按钮，打开“添加计数器”对话框，如图 15.7 所示。

在“添加计数器”对话框中，首先选择是“使用本地计算机计数器”还是“从计算机选择计数器”，如果是“从计算机选择计数器”，需要在下拉列表框中输入或指定一台网络计算机的名称。

然后在“性能对象”中选择要监控的对象。可使用的对象基于安装在计算机上的服务和应用程序，可以为每个对象选择多个计数器，其中，几个 Windows Servre 2003 系统监视器中的核心对象如下：

在“所有计数器”和“从列表选择计数器”单选按钮中选择计数器。单击“说明”按钮可以查看在“添加计数器”对话框列出的计数器的描述。

单击“添加”按钮，然后单击“关闭”按钮，完成计数器的添加。

如果要删除某个计数器，可先在“性能”窗口中选中该计数器，然后单击工具面板上的“删除”按钮。

步骤 6：设置标题和网格

选择“图表”选项卡，可将标题、网格和其他属性添加到图表。

步骤 7：性能日志和警报

可以使用性能日志和警报来对系统资源进行详细监视，当指标超出设定的标准时，可以使用警报来通知用户或系统管理员。

（1）建立计数器日志文件。使用性能日志和报警，首先要建立计数器日志，建立步骤如下：

在“性能”窗口双击展开“性能日志和报警”管理单元，右击“计数器日志”选项，选

择“新建日志设置”命令，弹出“输入新日志名称”对话框，输入名称后单击“确定”按钮，弹出“日志设置”对话框，如图 15.8 所示。

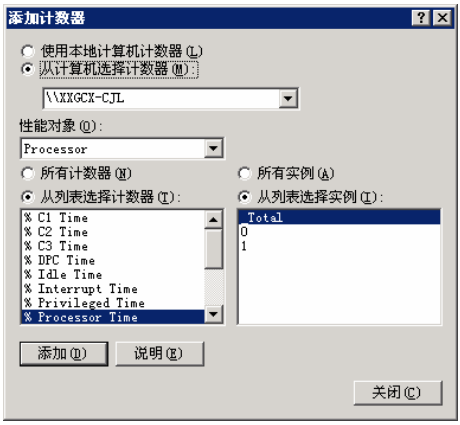

图 15.7 “添加计数器”对话框

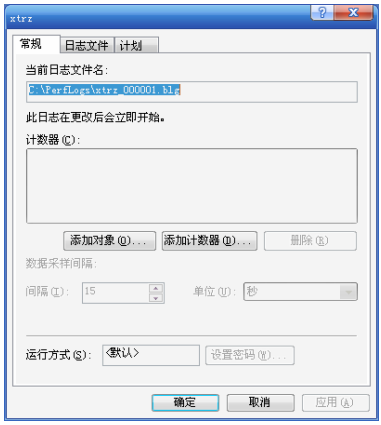

图 15.8 “日志设置”对话框

- “常规”选项卡：设置对象或计数器；
- “日志文件”选项卡：设置日志文件的格式；
- “计划”选项卡：设置记录日志的时间。

（2）建立警报。可以对一些需要监视的计数器设置警报，当警报发生时系统将信息传到网络上的某台计算机。这样，当系统管理员在网络上的其他计算机上工作时也可收到警报。

在“性能”窗口双击展开“性能日志和报警”管理单元，右击“警报”选项，选择“新建警报设置”命令，弹出“输入新警报名称”对话框，输入名称后单击“确定”按钮，弹出“警报设置”对话框，如图 15.9 所示。

- “常规”选项卡：让计数器在达到某一个限值时便发生警报，以提醒系统管理员；
- “操作”选项卡：设置当该事件发生后所要处理的事件或执行的程序；
- “计划”选项卡：设置启动报警的时间等。

15.2.2 使用“事件查看器”管理事件日志

事件是根据审核策略记录的用户行为，即在 Windows 或应用程序中发生的任何有重大意义的情况。监视事件可以标识和追踪安全事件、资源使用情况及系统和应用程序运行情况等。

Windows Server 2003 在运行之后会将许多重要的事件记录下来，这就是事件日志。系统管理员可以利用系统提供的“事件查看器”来查看与管理它们。这样在应用程序、服务或系统运行异常时，可以在此查看问题以排除异常情况。

选择“开始→程序→管理工具→事件查看器”命令，打开“事件查看器”窗口，如图 15.10 所示。

在“事件查看器”窗口左边窗格中是事件的分类，右边窗格是事件的详细信息。Windows 主要使用 3 种日志来记录事件。

- “应用程序”日志：该日志包含应用程序或其他程序记录的事件。
- “安全性”日志：该日志根据审核策略记录安全事件，如无效或有效地登录等；
- “系统”日志：该日志包含 Windwos 系统组件记录的事件，如驱动器或其他组件启

动时如果失败会被记录在该日志中。

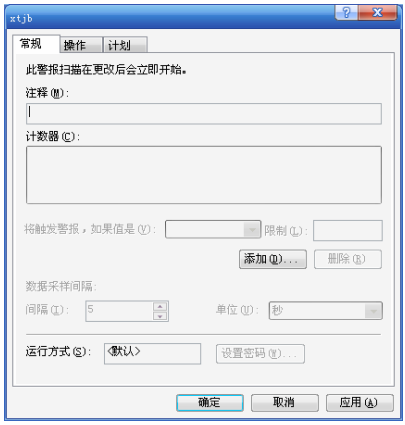

图 15.9 “警报设置”对话框

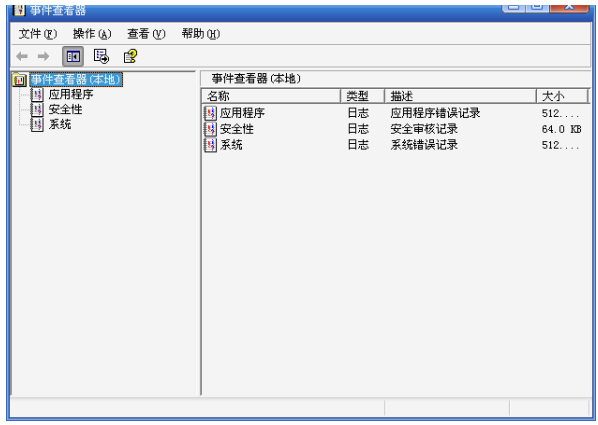

图 15.10 “事件查看器”窗口

所有用户可以查看应用程序日志和系统日志，但只有系统管理员才能查看安全事件。

如果要查看某个事件的详细信息，可以双击该事件，打开“警告属性”对话框，查看引发该事件的一些详细信息。

步骤 1：筛选和查找事件

Windows 事件查看器通过设置筛选条件可以找到某些特定的事件。操作步骤如下：

（1）打开“事件查看器”窗口，在左边窗格中选择一个要进行筛选的事件分类，如“安全性”，在右边的窗格中会列出该类事件的信息。执行“查看→筛选”命令，打开“筛选器”对话框，如图 17.11 所示。

（2）在“筛选器”选项卡中，分别选择筛选的事件类型、事件来源、类别、事件 ID、用户、计算机及事件的起始时间等条件。

筛选后，事件窗口中将只显示满足筛选条件的事件。

同样，可以使用查找的方法来搜索特定事件，执行“查看→查找”命令，打开“查找”对话框，和“筛选器”类似，在这里不再叙述。

步骤 2：清除和保存事件日志

为了使事件日志不占用过多的系统资源，可以对其进行相应的整理，如清除或存档等。清除或保存事件日志的步骤如下：

（1）打开“事件查看器”窗口，在左边窗格中选择一个要进行筛选的事件分类，例如“安全性”日志，执行“操作→清除所有事件”命令，此时系统弹出对话框询问是否要保存事件，单击“否”，直接清除安全性日志。

（2）如果单击“是”，将弹出“将 安全性 另存为”对话框，可以用来保存日志。这与通过执行“操作→另存日志文件”命令是一样的。事件日志通常有 3 种存储格式：

- 日志文件格式（.evt）：默认格式，用户可在事件查看器中调用查看；
- 文本文件格式（.txt）：以制表位分割的文本文件，用户可以通过文字处理程序调用查看；
- 逗号分隔文本格式（.csv）：具有分隔符的文本文件，可以通过电子表格或数据库等程

序调用查看。

以文本文件格式（.txt）或逗号分隔文本格式（.csv）保存的日志不保留事件中的二进制数据。

也可以选择“操作→导出列表”命令来保存事件日志。

步骤 3：打开事件日志

如果要查看已存档的事件日志，可以调用相应的程序查看。

执行“操作→打开日志文件”命令，弹出“打开”对话框，在对话框中选中一个日志文件。

事件查看器只能查看日志文件格式（.evt）。

也可以使用“记事本”查看文本文件格式（.txt）的事件日志，用 Excel 查看逗号分隔文本格式（.csv）的事件日志。

步骤 4：限制事件日志容量

可以限制事件日志的容量，或者利用新事件日志覆盖已过时事件日志，以节省磁盘空间。

（1）打开“事件查看器”窗口，在左边窗格中选择一个要进行筛选的事件分类，例如“安全性”日志，执行“操作→属性”命令，此时弹出“安全性 属性”对话框，如图 15.12 所示。

图 15.11 “筛选器”对话框

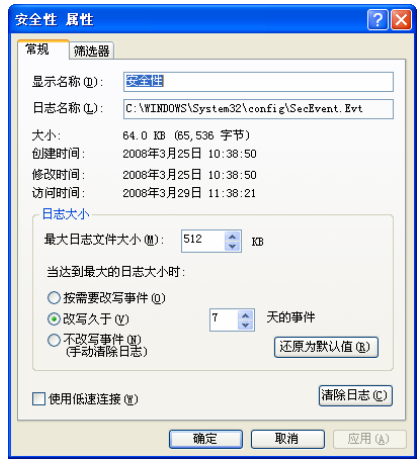

图 15.12 “常规”对话框

（2）在“常规”选项卡的“最大日志文件大小”中输入日志最大容量，单位“KB”。当日志文件达到规定的存储值时，有 3 个选项可选：按需要改写、改写久于×天以前的事件、不改写事件。

15.2.3 使用“任务管理器”监视系统资源

“任务管理器”是 Windows Server 2003 中一个用来监视系统运行情况的实用工具，通过“Windows 任务管理器”，管理员可以查看当前在计算机上运行的各种应用程序的实时信息以及进程和内存使用的情况。

步骤 1：启动“任务管理器”

在 Windows 桌面上，按下 Ctrl+Alt+Del 组合键，弹出“Windows 安全”对话框，单击“任

务管理器”按钮，即可启动任务管理器，如图 15.13 所示。如果不小心接连按了两次键，可能会导致 Windows 系统重新启动。

也可以右击“任务栏”的空白处，然后单击“任务管理器”命令。或者，按下“Ctrl+Shift+Esc”组合键，也可以打开任务管理器。

“任务管理器”窗口提供了文件、选项、查看、窗口、关机、帮助 6 个菜单项。例如，“关机”菜单下可以完成待机、休眠、关闭、重新启动、注销、切换等操作，其下还有应用程序、进程、性能、联网、用户 5 个标签页，窗口底部则是状态栏，从这里可以查看到当前系统的进程数、CPU 使用比率、更改的内存“容量”等数据，默认设置下系统每隔 2 秒钟对数据进行一次自动更新，也可以通过“查看→更新速度”菜单重新设置。

1）监视应用程序

“应用程序”标签中显示了所有当前正在运行的应用程序的状态，不过它只会显示当前已打开窗口的应用程序，而最小化至系统托盘区的应用程序则不会显示出来。

可以在这里单击“结束任务”按钮直接关闭某个应用程序，如果需要同时结束多个任务，可以按住 Ctrl 键复选；单击“新任务”按钮，可以直接打开相应的程序、文件夹、文档或 Internet 资源，如果不知道程序的名称，可以单击“浏览”按钮进行搜索。

2）监视进程

“进程”标签显示了所有当前正在运行的进程的信息，如图 15.14 所示，其中包括 CPU 和内存使用情况、页面错误、句柄计数及其他一些参数等。那些隐藏在系统底层深处运行的病毒程序或木马程序都可以在这里找到，当然前提是要知道它的名称。如果要结束某个进程，可先选中该进程，然后单击“结束进程”按钮，就可以强行终止；如果要结束某进程及由该进程直接或间接创建的所有进程，可右击该进程，然后在弹出的快捷菜单中选择“结束进程树”命令。

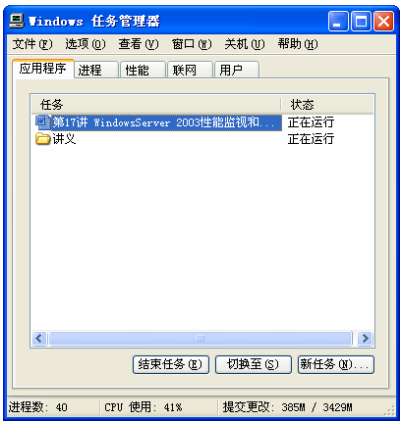

图 15.13 “任务管理器”窗口

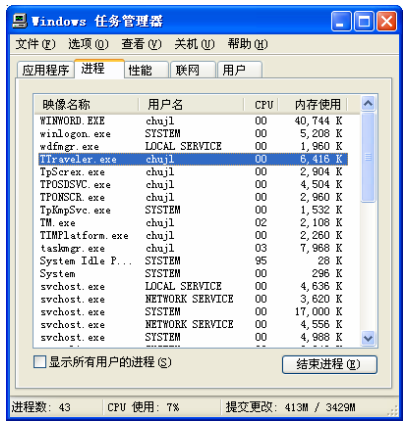

图 15.14 “进程”标签

Windows 的任务管理器只能显示系统中当前进行的进程，而 Process Explorer 可以树状方式显示出各个进程之间的关系，即某一进程启动了哪些其他的进程，还可以显示某个进程所调用的文件或文件夹。如果某个进程是 Windows 服务，则可以查看该进程所注册的所有服务。

3）监视性能

“性能”标签中记录了计算机的性能概况，其中包括 CPU 和各种内存的使用情况。在计

算机上运行的句柄数和线程数等。如图 15.15 所示。

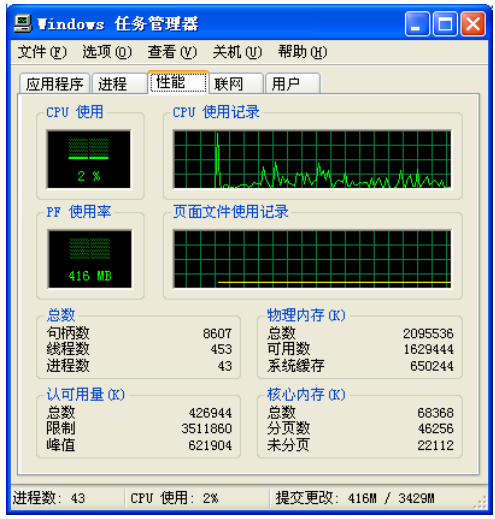

图 15.15 “性能”标签

- CPU 使用情况：表明处理器工作时间百分比的图表，该计数器是处理器活动的主要指示器，查看该图表可以知道当前使用的处理时间是多少。
- CPU 使用记录：显示处理器的使用程序随时间的变化情况的图表，图表中显示的采样情况取决于“查看”菜单中所选择的“更新速度”设置值，“高”表示每秒 2 次，“正常”表示每 2 秒 1 次，“低”表示每 4 秒 1 次，“暂停”表示不自动更新。
- PF 使用情况：正被系统使用的页面文件的量。
- 页面文件使用记录：显示页面文件的量随时间的变化情况的图表，图表中显示的采样情况取决于“查看”菜单中所选择的“更新速度”设置值。
- 总数：显示计算机上正在运行的句柄、线程、进程的总数。
- 执行内存：分配给程序和操作系统的内存，由于虚拟内存的存在，“峰值”可以超过最大物理内存，“总数”值与“页面文件使用记录”图表中显示的值相同。
- 物理内存：计算机上安装的总物理内存，也称 RAM，“可用数”表示可供使用的内存容量，“系统缓存”显示当前用于映射打开文件的页面的物理内存。
- 内核内存：操作系统内核和设备驱动程序所使用的内存，“页面”是可以复制到页面文件中的内存，由此可以释放物理内存；“非分页”是保留在物理内存中的内存，不会被复制到页面文件中。

4）监视网络

使用“任务管理器”还可以查看网络状态，在“联网”标签中显示了适配器的状态，包括当前适配器流量使用情况、网络速度和应用状态等。

5）监视用户

“用户”标签记录了当前登录系统的域用户的状态。可以选择某个用户，单击“断开”按钮来断开该用户，也可单击“注销”按钮注销该用户。

步骤 2：“任务管理器”的使用

其实，任务管理器除了终止任务、结束进程、查看性能外，它还可以完成很多更高级的

特别任务。下面，通过几个实例来介绍任务管理器的扩展应用。

实例一：同时最小化多个窗口

切换到“应用程序”标签页，按住 Ctrl 键选择需要同时最小化的应用程序项目，然后右击这些项目中的任意一个，从菜单中选择“最小化”选项即可。同时还可以完成层叠、横向平铺、纵向平铺等操作。

实例二：降低 BT 软件的资源占用率

运行 BT 软件时，往往会占用大量的系统资源，硬盘灯会不停闪烁并伴随着飞速转动的噪声，此时无论是浏览网页或是运行其他应用程序，都会有系统停滞的感觉。

打开“任务管理器→进程”窗口，选择 BT 软件的进程名，然后从右键菜单中选择“设置优先级”选项，这里可以选择实时、高、高于标准、标准、低于标准、低等不同级别，可根据实际情况进行设置。例如，设置为“低于标准”可以降低进程的优先级别，从而让 Windows 为其他进程分配更多的资源。

实例三：打造增强版本的任务管理器

可以从 Longhorn 中将任务管理器剥离出来并提供下载，从而打造一个增强版本的任务管理器。解压缩下载文件，会得到 Taskkill.exe、Tasklist.exe、Taskmgr.exe 3 个文件，首先覆盖\Windows\System32\Dllcahe\下的同名文件，覆盖前要备份源文件，接下来继续覆盖\Windows\System32\下的同名文件，当弹出“Windows 文件保护”对话框时，单击“取消”按钮。

更换后的任务管理器不仅程序图标发生了变化，右击进程，可以发现在右键菜单中增加了“打开所在目录”、“创建转储文件”2 个选项，而“查看→选择列”中增加了“命令行”、“映像路径”2 个选项，前者可以查看所显示的进程是否被伪装，后者可以查看进程的文件路径。

实例四：打开处理器的超线程

P4 处理器的超线程技术（Hyper-Threading Technology）相当于将一个处理器分为两个虚拟的处理器，简单地说，实现超线程需要处理器、主板、操作系统三方面的支持。如果使用的是 Windows XP/Server 2003，而且确定自己的主板和处理器支持超线程，那么可以切换到“性能”标签页，如果这里显示两个 CPU 使用记录图表的话，说明处理器已经打开超线程。

当然，也可以在开机信息中查看超线程支持情况，一般会显示 CPU1、CPU2 两个处理器名称，或者启动后进入“设备管理器”，同样会显示两个处理器的信息。

实例五：禁用任务管理器

如果使用的是公用计算机，而又不希望他人私自操作任务管理器，可以在“开始→运行”中输入“gpedit.msc”命令，打开组策略窗口，找到“本地计算机策略→用户配置→管理模板→系统→Ctrl+Alt+Del 选项”项，然后在右侧窗口中选择“删除任务管理器”项，将其设置为“已启用”，这样当以后按下“Ctrl+Alt+Del”组合键时就无法启用任务管理器了。

习　题

一、思考题

1．简述使用任务管理器结束进程步骤？

2．要查看处理器使用情况，应该使用哪个计数器？

3．某用户的Word程序停止响应了，什么工具可以帮助他确定Word是否还在运行？如果没有运行该怎样停止任务？

4．如何安装网络监视器管理工具？

二、实训题

1．网络性能监视器的设置。

（1）利用 Windows Server 2003 自带的网络诊断工具监视网络的利用率、每秒帧数、每秒字节数、每秒的广播和多播？

（2）创建捕获筛选程序，捕获与指定机器之间的数据包。

（3）创建捕获筛选程序，捕获计算机基于 IP 协议的数据包。

（4）创建一触发器，设置满足一定条件时停止捕获。

参考文献

［1］IT 同路人．非常网管 Windows Server 2003 服务器架设实例详解．北京：人民邮电出版社，2008.

［2］朱元忠，方园．网络操作系统案例教程．北京：机械工业出版社，2008.

［3］梁锦锐．Windows 组网技术实训教程．北京：清华大学出版社，2007.

［4］李馥娟．计算机网络实验教程．北京：清华大学出版社，2007.

［5］黄崇本．操作系统实用教程——Windows 2003．北京：高等教育出版社，2008.

［6］唐华．Windows Server 2003 系统管理与网络管理．北京：电子工业出版社，2006.

［7］鞠光明．Windows 服务器维护与管理教程与实训．北京：北京大学出版社，2005.

［8］冯胜安．网络操作系统——Windows Server 2003 系统与应用．北京：电子工业出版社，2008.

［9］魏茂林．Windows Server 2003 网络服务器管理与使用．北京：电子工业出版社，2007.

［10］韩清．网络操作系统——Windows Server 2003 管理与应用．北京：清华大学出版社，2008.

［11］王国全．Windows Server 2003 配置与管理．北京：清华大学出版社，2008.

［12］王达．网管第一课——网络操作系统与配置管理．北京：电子工业出版社，2008.